LUXOFT GROUP DATA PROTECTION POLICY

CONTENTS

Part One: General_____ **Page 3**

Data Protection Policy: Requirements for all Luxoft Group Staff

Part Two: Department or country specific guidance_____ **Page 11**

PART ONE: GENERAL

LUXOFT GROUP DATA PROTECTION POLICY

REQUIREMENTS FOR ALL STAFF

1. **PURPOSE**

1.1 This document sets out the policies and procedures that the LUXOFT GROUP has put in place to comply with basic data protection principles. Since a number of entities of the LUXOFT GROUP are situated in Europe, this document especially takes into account European data protection laws and provides a short overview of these laws – especially the European Data Protection Directive (Directive 95/46/EC) respectively the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") from 25 May 2018 onward.

2. **SCOPE**

2.1 This policy applies to Luxoft Holding, Inc. and all of its branches and entities worldwide (together "**LUXOFT GROUP**"). All employees and agency personnel (staff) within LUXOFT GROUP must comply with the policy. All LUXOFT GROUP staff will receive information security training (which includes data protection compliance) on a regular basis.

2.2 Some parts of this policy apply to the branches and entities situated in EU or EEA countries respectively Switzerland ("**European Operations**") only.

2.3 This policy is split into two parts: Part One is general and applies to all staff. Part Two contains additional provisions for specific departments and operations in specific countries. More detailed provisions apply to:

- Annex A: Personnel Department;
- Annex B: Delivery and Procurement;
- Annex C: Information Technology;
- Annex D: Facilities; and
- Annex E: Legal.

2.4 Data protection laws vary from country to country. This policy has been reviewed for local compliance in Australia, British Virgin Islands, Bulgaria, Canada, China, Cyprus, Denmark, Italy, India, France, Germany, Luxembourg, Malaysia, Mexico, The Netherlands, Poland, Romania, Russia, Singapore, Sweden, Switzerland, UK, Ukraine, USA, Korea and Vietnam. Where there is a different requirement in these countries, a note is indicated above the text and you must refer to the relevant country-specific Appendix in Part Two.

3. **COMMITMENT TO COMPLY WITH BASIC DATA PROTECTION PRINCIPLES**

3.1 All LUXOFT GROUP staff must comply with their obligations under this policy and applicable local data protection laws whenever they are processing personal data **[China 1]**. The Data Protection Safeguards set out in Section 4 below and in Part Two set out what this means.

3.2 **Data protection principles apply when personal data is processed by, or on behalf of, LUXOFT GROUP.**

3.3 'Personal data' means, without limitation: personally identifiable information or personal data as defined under the laws of the respective jurisdiction, including the EU Regulation (EU) 2016/679 ("GDPR"); and in any event (i) any information that can be used to distinguish or trace an individual's identity, such as person's name, date and place of birth, biometric records, mother's maiden name, address, email address, telephone number, social security number, state identification or driver's license numbers, account information, PIN numbers, access and security codes, login information; and (ii) any other information that is linked or linkable to an individual, such as information about a person's sex, age, income, health or medical information, educational, financial and employment information. Personal Information includes whole or partial copies of such information or materials derived from such information. **[Australia 1] [Bulgaria 1] [China 1] [Denmark 1] [Luxembourg 1] [Malaysia 1] [Singapore 1] [Switzerland 1][Korea 1]**

3.4 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal data transmitted, stored or otherwise processed.

3.5 'Processing' also has a broad meaning: for example, it covers collection of data, holding and using data and destroying personal data. All LUXOFT GROUP staff will almost certainly process some personal data: about clients or suppliers, or about other employees.

3.6 'Processor' means the natural or legal person which processes personal data on behalf of the controller.[Korea 3]

3.7 'Controller' means the natural or legal person which alone or jointly with others, determines the purposes and means of the processing of personal data. **[Korea 3]**

3.8 Basic data protection principles require that LUXOFT GROUP:

- only processes personal data for fair and lawful purposes; **[France 1]**
- in accordance with additional restrictions for sensitive personal data[1]; **[China 2][Korea 2]**
- is transparent with people and tells them how it will use their information;
- meets data quality obligations and holds personal data for a limited retention period;
- as a general rule minimises the amount of personal data it collects **[Denmark 2]** and processes and chooses and structures its processing systems accordingly; **[France 2]**
- as a general rule grants its staff access to personal data on a "need to know" basis only;
- implements appropriate security obligations to protect personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;
- upholds individuals' rights to access and correct their information and, to prevent certain types of processing; **[Denmark 3] [France 3] [Mexico 1] [Sweden 1]** and
- only transfer personal data to other jurisdictions than their own when protections for personal data are in place as required by local law (e.g. European Operations only transfer personal data out of the European Economic Area (EEA)[2] and Switzerland when protections for personal data are in place such as the standard contractual clauses provided by the EU Commission). **[India 6 and India 7] [China 3] [Malaysia 2] [Switzerland 1]**

3.9 Data protection laws often also require that LUXOFT GROUP must notify its processing of personal data to the local data protection authority. The appropriate Data Protection Officer is responsible for ensuring that this is done. **[Australia 2] [China 4] [Denmark 4] [India 2] [France 4] [Luxembourg 2] [Malaysia 3] [Ukraine 1]**

3.10 Section 4 sets out the steps LUXOFT GROUP has adopted and that you must follow to ensure that these obligations are met.

4. DATA PROTECTION SAFEGUARDS

4.1 Lawful purposes

4.1.1 LUXOFT GROUP may only process personal data for explicit and legitimate purposes and does not further process data in a manner that is incompatible with those purposes. **[France 1] [Vietnam 1]**

4.1.2 Luxoft may process ordinary personal data only based on the following grounds:

- the data subject has explicitly and freely given his\her consent (for one or more specific purposes) or has been duly notified;

[1] For a definition of sensitive personal data see 4.2 below.
[2] EU Member States, Norway, Iceland, and Liechtenstein.

- the data processing is necessary to enter into or to perform a contract which the data subject is a party or in order to take steps at the request of the individual prior to entering into a contract;
- the processing is necessary to comply with a legal obligation **[Bulgaria 2] [Denmark 5] [Singapore 2] [Vietnam 2]**;
- the processing is necessary in order to protect the vital interests of the data subject;
- the processing is necessary for the performance of a request of public authority (i.e. government);
- the processing is necessary for the purposes of the LUXOFT GROUP's legitimate interests (as defined by local law), provided this does not cause unreasonable prejudice to the interests of the individuals concerned. **[China 5] [Cyprus 1] [Sweden 2] [Cyprus 1] [Sweden 2].**

In the case of any doubt, you should seek guidance from the Data Protection Officer.

4.1.3 In some situations, LUXOFT GROUP may also process personal data when the relevant individual has given consent. This must usually be express and in many countries this is subject to strict formal requirements. Marketing may process personal data on this basis. In other situations, staff should seek guidance from the Data Protection Officer if they wish to collect and use personal data based on individual consent. **[Canada 1] [India 2, India 3, India 4 and India 5] [France 5] [China 6] [Malaysia 3 and Malaysia 4] [Russia 1][Korea 2]**

4.1.4 Where LUXOFT GROUP holds personal data for certain specific purposes, staff must not then use the data any other way which is incompatible with those purposes: if the relevant individuals would not expect this use of the data, it is likely to be 'incompatible use'. For example, you may not access the client or staff databases for your own purposes, or for friends or family. This is a serious disciplinary offence and may be a criminal offence for which you can be prosecuted.

4.1.5 Use of data for a new purpose, can also affect LUXOFT GROUP's filings with data protection authorities. Staff must therefore consult the Data Protection Officer, if they wish to use personal data for a new purpose. **[India 2 and India 3] [France 6] [Malaysia 3] [Mexico 2]**

4.2 Sensitive personal data

4.2.1 Sensitive personal data is generally information about an individual's physical or mental health or condition, racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs and sexual life, genetic and biometric data (if this data is processed for the purpose of uniquely identifying an individual) although local laws may vary (for example in the UK, the commission or alleged commission of any criminal offence and criminal convictions are also sensitive personal data and in Poland sensitive personal data includes data relating to decisions issued in court or administrative hearings). **[Australia 3] [Bulgaria 3] [Canada 2] [China 2] [Cyprus 2] [Denmark 6] [India 1France 7] [Luxembourg 3] [Malaysia 5] [Netherlands 1] [Russia 2] [Ukraine 2] [Korea 2]**

4.2.2 Personnel Department is the only department where staff is allowed to process sensitive personal data. **[France 8] [Ukraine 3]**

4.3 Transparency

4.3.1 LUXOFT GROUP must be transparent about how it uses personal data: if you collect personal data about individuals, you must tell them how this information will be used. This means providing information about **[Australia 4] [France 9] [Malaysia 6]**:

- the LUXOFT GROUP entity collecting the information (including the contact data of the Data Protection Officer, where applicable); **[Bulgaria 4] [Denmark 7] [Poland 1] [Sweden 3] [Ukraine 4]**
- the purposes for which LUXOFT GROUP processes personal data as well as the legal basis for the processing; **[Vietnam 3]**
- where the data processing is based on legitimate interests, the legitimate interests of LUXOFT GROUP on which the data processing is based;
- whether replies to questions are mandatory or voluntary, and the consequences if information is not provided;
- the types of people who will receive the data and the purposes for which they will receive it;
- the rights that individuals have (including to access, correct and sometimes to object to the processing of their data) **[Denmark 3] [Sweden 1]**; and

- any transfers of personal data outside their own jurisdiction, where required by local law; European Operations have to provide information about any transfers of personal data outside EEA. **[Australia 5] [Canada 3] [China 3] [Denmark 8] [India 6 and India 7] [France 10) [Switzerland 1] [Russia 3] [Ukraine 5].**

4.3.2 In addition to the information referred to in Section 4.3.1, the LUXOFT GROUP shall, at the time when personal data are obtained, provide individuals with the following further information necessary to ensure fair and transparent processing in accordance with applicable data protection laws:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from LUXOFT GROUP access to and rectification or erasure of personal data or restriction of processing concerning individuals or to object to processing as well as the right to data portability;
- if the data processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether an individual is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for an individual;

4.3.3 Where personal data has not been directly obtained from an individual, and in accordance with applicable data protection laws, the LUXOFT GROUP shall provide the individual with the following information in addition to the information as set out in 4.3.2:

- the categories of personal data concerned;
- from which source the personal data originate, and if applicable, whether it comes from publicly accessible sources.

4.3.4 In general, the information set out under the foregoing sections must be provided to individuals before LUXOFT GROUP obtains personal data from them. LUXOFT GROUP does not have to provide this information to the extent the individual already has the information. Specific requirements for Personnel Department and Marketing are set out in the relevant Annexes **[France 11]**.

4.3.5 It is not necessary to provide this information for business contact information provided by the individual, where it is evident from the context how you will use the information (e.g. giving a card to allow for follow up). **[Australia 6] [Bulgaria 5] [Canada 4] [China 7] [Denmark 9] [France 12] [Luxembourg 4] [Malaysia 7] [Poland 2] [Switzerland 2]**

4.4 Data quality and retention

4.4.1 You should only use personal data that is adequate, relevant and not excessive. Data may only be collected if there is a business need for the information and if the level of information is proportionate to this.

4.4.2 You should use personal data that is accurate and, where necessary, up to date. You should advise the Personnel Department promptly if your details change. If you are told about a change in a client's or supplier's personnel, you should change any local contact databases that you maintain and ensure central databases are updated accordingly.

4.4.3 LUXOFT GROUP must not retain personal data for longer than is necessary for the purposes for which the data was collected. Guidance on what this means for Personnel Department is set out in Annex A **[China 8]**.

4.5 Security and Confidentiality

4.5.1 LUXOFT GROUP shall implement appropriate administrative, technical, organisational and physical measures to protect personal data, including *but not limited*,

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a data breach;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.5.2 This requires appropriate IT and physical security measures and staff training and care in selection of third parties who process LUXOFT GROUP personal data. These measures may vary from country to country.

4.5.3 LUXOFT GROUP shall, where required and in accordance with applicable laws, carry out data protection impact assessments ("DPIA") **before introducing** new processing operations.

4.5.4 PLEASE NOTE that before the starting of any new project involving personal data, project manager must **always involve the Data Protection Officer** to conduct a Privacy Impact Assessment and Legitimate Interest Assessment.

4.5.5 The main processes for securing the LUXOFT GROUP IT environment are set out in the Information Security Manual, Security Incident Management policy and associated documents, which all staff must comply with. Further guidelines are set out in the Corporate Code of Conduct, the Insider Trading Policy, the Rules for Handling of Service Information, the Regulations on the Processing of Personal Data, Rules on Company Information Treatment by Employees, Instructions "Use of Corporate Electronic Mail" and Non-disclosure agreements.

4.5.6 Where staff have permission to work from home or any other off-premises site, special conditions apply to the handling of personal data which must be fully observed.

4.5.7 Any suspected or actual data breach ("security incident", "data leak"), unauthorised loss or disclosure of, access or damage to, misuse or of any LUXOFT GROUP personal data (including loss of or damage to equipment containing LUXOFT GROUP personal data) shall be reported immediately in ServiceDesk system. It is obligatory for all employees to use ServiceDesk system for security incident reporting. **[China 9] [Denmark 10] [India 2 and India 8] [Malaysia 3]**

4.5.8 The Personal Data Breach shall be investigated as prescribed by the Security Incident Management policy.

4.5.9 Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the individual and the legitimacy of the request according to LUXOFT GROUP's policies, particularly before releasing information over the phone. If in doubt, please speak to the appropriate Data Protection Officer.

4.6 **Restriction on transfers outside the EEA** **[Australia 7] [China 3] [Denmark 11] [India 6 and India 7] [Malaysia 2]**

4.6.1 European data protection rules restrict transfers of personal data to including group companies in countries that are outside the European Economic Area (EEA)[3] and Switzerland unless prescribed steps are taken to ensure that the data is protected. Since some of LUXOFT GROUP's IT applications are held and backed outside the EEA and Switzerland, this restriction is particularly relevant for its European Operations. **[Singapore 3] [Switzerland 1]**

4.6.2 LUXOFT GROUP has put in place European Commission approved agreements to regulate the transfers of certain categories of data within the LUXOFT GROUP of companies. **[China 10] [Singapore 4] [Switzerland 1]**

4.6.3 European Operations staff must seek the input of the Data Protection Officer if you want to transfer personal data to a new supplier outside the EEA or Switzerland or if you want to transfer new categories of data to LUXOFT GROUP entities outside the EEA or Switzerland. The input of the Data Protection Officer must include the information whether prior notification or authorisation of the transfer by the competent data protection authority is required. **[Cyprus 3] [Singapore 5]**

[3] EU Member States, Norway, Iceland, and Liechtenstein.

4.7 Rights of Individuals

4.7.1 Each individual shall have the right to obtain from LUXOFT GROUP confirmation as to whether or not personal data concerning the individuals is processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from LUXOFT GROUP rectification or erasure of personal data, restriction of processing personal data concerning the individual, and to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where personal data is not collected directly from the individual, any available information as to their source;
- the existence of automated decision-making, including profiling.

4.7.2 Where personal data is transferred to a third country or to an international organisation, the individual shall have the right to be informed of the appropriate safeguards relating to the transfer.

4.7.3 LUXOFT GROUP will always honour individuals' rights under and according to data protection laws:

- correct information relating to them;**[Denmark 3] [France 3] [Sweden 1] [Vietnam 4]**
- to erasure ("right to be forgotten");
- to data portability;
- to restriction of processing;
- to prevent direct marketing to them; **[France 13]**
- to prevent certain other types of processing in special situations; and
- to object to the use of entirely automated decisions to take significant decisions about them. **[China 11] [Mexico 3] [Russia 4]**

4.7.4 Staff must take care when entering information in free-text areas as those to whom the text refers (such as clients) may see this information at a later date. Information should only be entered which is appropriate and justifiable and should not include sensitive personal data.

4.7.5 Requests by staff to see their records should be made, in writing, to the Head of Personnel Department. If staff receives any other request to see personal details or a request that LUXOFT GROUP delete data or cease processing data should be forwarded immediately to the Data Protection Officer. There are often strict timescales for complying with such requests, so requests must be forwarded as soon as possible following receipt. **[India 2] [Malaysia 3] [Sweden 4]**

4.8 Place where decisions about the purpose and means of the processing activities are taken

4.8.1 With regard to personal data of employees and customers of Luxoft entities situated in Europe being subject to cross-border processing activities pursuant to Art. 4 No. 23 GDPR, Luxoft GmbH (Stadionstrasse 66, 70771 Leinfelden-Echterdingen, Germany) is the entity where decisions about the purpose and means of the processing activities are taken.

4.8.2 Luxoft GmbH is involved in shaping strategic group-wide decisions with data protection relevance and will in particular:

- oversee data protection related implications of cross-border processing activities in conjunction with the Global Data Protection Officer and takes the final decisions about the purposes and means of cross-border processing activities;
- in coordination with the Global Data Protection Officer, be responsible for carrying out data protection audits;
- co-manage complaint handling processes together with the Global Data Protection Officer;
- provide guidance and training on data protection compliance together with the Global Data Protection Officer, e.g. by creating and circulating information material and carrying out training sessions;

- be vested with directional rights as needed to fulfil the tasks set out above, including the right to instruct other Luxoft Group entities to demonstrate compliance with data protection law;
- take a lead role for communicating the data protection requirements within the group and for ensuring compliance with these standards.

4.9 Data protection rules of contracting

4.9.1 Lawyers should always clarify the essence of relations with the client/supplier, determine who is a data controller and who is a data processor, review the contract in LuxContract carefully and strictly follow the following rules of data protection in contracting:

FOR CLIENTS:

4.9.2 If Luxoft's assigned personnel may have unintended access to the client's personal data, without any further processing of it, then please amend the contract with a special data protection wording (please see the sample in the Annex E, Supplementary document 4).

4.9.3 If Luxoft processes personal data of the client on Luxoft's computers and servers, then please initiate the signing of a Data Processing Agreement with the client (please see the sample in the Annex E, Supplementary document 5). If the client is located in the EEA and data are transferred to or accessed from outside the EEA, please use Standard contractual clauses under DPO instructions.

FOR SUPPLIERS:

4.9.4 If supplier's assigned personnel may have unintended access to personal data without any further processing of it, then please amend the contract with special data processor wording (please see the sample in the Annex E, Supplementary document 6).

4.9.5 If supplier processes personal data of Luxoft (e.g. personal data of employees or customers of Luxoft) under Luxoft documented instructions and on behalf of Luxoft ("Controller-to-Processor" transfer), Luxoft must enter into a data processing agreement with the supplier (please see the sample in the Annex E, Supplementary document 7).

4.9.6 If supplier processes personal data of Luxoft's client on supplier's computers and servers then please initiate the signing of Data Sub-Processing Agreement with supplier (please see the sample in the Annex E, Supplementary document 8).

4.9.7 If supplier processes personal data of Luxoft (e.g. personal data of employees or customers of Luxoft) as a data controller ("Controller-to-Controller" transfer), **no data processing agreement between Luxoft and supplier is required.**

4.9.8 If suppliers are located outside the EEA and personal data will be transferred to or accessed from outside the EEA, please use Standard Contractual Clauses under DPO instructions.

4.9.9 **In case of any doubt about the necessary document or essence of the relations, you should seek guidance from the Global DPO.**

5. EXCEPTIONS:

Any request to deviate from this policy must be approved by the DPO. **[India 2] [Malaysia 3]**

6. VIOLATIONS:

6.1 Subject to local law requirements, failure to comply with this policy may be a disciplinary offence and will be handled in accordance with LUXOFT GROUP's disciplinary procedures.

6.2 Failure to comply with this policy may also mean that you are directly liable for penalties under local data protection law. In particular, use, for private or illegal purposes, of personal data obtained through your work at LUXOFT GROUP can be a criminal offence. **[France 14] [Ukraine 6]**

7. ANY QUERIES?

If you have any queries in relation to this policy or data protection generally, you should contact you're a Global Data Protection Officer: GlobalDataProtectionOffice@luxoft.com. **[India 2] [Malaysia 3]**

8. APPROVAL AND VARIATION

This policy has been approved by Board of Directors of Luxoft Holding Inc. The Data Protection Officer is the sponsor for this policy and must approve any changes to it. **[India 2] [Malaysia 3]**

PART TWO: DEPARTMENT OR COUNTRY SPECIFIC GUIDANCE

CONTENTS

ANNEXES

Annex A: **Personnel Department**

Supplementary Document 1: **Sample Consent to the Processing of Personal Data**

Supplementary Document 1.1: **Sample Data Protection Notice for Applicants-Online form**

Supplementary Document 2: **Sample Privacy Notice for Employees**

Supplementary Document 3.1: **General Records Retention Periods for intercompany databases**

Supplementary Document 3.2: **Personnel Department Records Retention Periods**

Annex B: **Delivery and Procurement**

Annex C: **Information Technology**

Annex D: **Facilities**

Annex E: **Legal**

Supplementary Document 4: **Sample Data Wording for MSA and NDA**

Supplementary Document 5: **Sample Data Processing Agreement with the Client**

Supplementary Document 6: **Sample Data Processor Wording with the Supplier**

Supplementary Document 7: **Sample Data Processor Agreement with the Supplier**

Supplementary Document 8: **Sample Data Sub-Processing agreement**

COUNTRY APPENDICES

(i) **Australia**

(ii) **Bulgaria**

(iii) **Canada**

(iv) **China**

(v) **Cyprus**

(vi) **Denmark**

(vii) **India**

(viii) **Italy**

(ix) **France**

(x) **Germany**

(xi) **Hong Kong**

(xii) **Luxembourg**

(xiii) **Malaysia**

(xiv) Mexico

(xv) The Netherlands

(xvi) Poland

(xvii) Romania

(xviii) Russia

(xix) Singapore

(xx) Sweden

(xxi) Switzerland

(xxii) UK

(xxiii) Ukraine

(xxiv) USA

(xxv) Vietnam

(xxvi) Korea

ANNEX A: PERSONNEL DEPARTMENT

DATA PROTECTION SAFEGUARDS

LAWFUL PURPOSES

Normal data

Some of LUXOFT GROUP's contracts of employment currently ask for employee consent to data processing. However, in most countries LUXOFT GROUP is entitled to process information about applicants and employees where: it is necessary for its legitimate interests; this is required to meet statutory obligations or to administer the employment contract. **[China 5] [Denmark 12] [France 15] [Germany 1] [Luxembourg 5] [Malaysia 8] [Mexico 4] [Netherlands 2-3] [Poland 3] [Russia 1] [Sweden 5] [Ukraine 7] [Vietnam 5]**

Sensitive data

LUXOFT GROUP is entitled to process sensitive personal data about employees where this is necessary to comply with obligations under employment law – such as dealing with statutory sick pay, or making work-place adjustments**. [India 3, India 4] [China 2 and China 5]**

Keep sickness and accident records separate from absence records, so absence records do not contain sensitive personal data. **[Bulgaria 6] [Cyprus 4] [Poland 4] [Romania 1]**

Criminal offences

Do not ask applicants for details of criminal offences unless this is necessary for the position. Generally, only unspent convictions will need to be requested. **[Cyprus 5] [France 16]**

Seek local advice before asking for criminal offence data outside the UK. **[Australia 8] [Canada 5] [Cyprus 6] [Denmark 13] [Germany 2] [Luxembourg 6] [Poland 5] [Romania 2] [Russia 2] [Sweden 6] [Switzerland 3] [Ukraine 8] [USA 1]**

New Uses

Use of data for a new purpose, can also affect LUXOFT GROUP's filings with data protection authorities (e.g new Personnel Department database or system). It may also require consultation with workers' representatives. Staff must therefore consult the Data Protection Officer, if they wish to use personal data for a new purpose. **[Bulgaria 7] [India 2] [France 6] [India 3] [France 17] [China 4] [Malaysia 3] [Mexico 5] [Netherlands 2-3][Singapore 6] [Ukraine 9]**

TRANSPARENCY

Applicants

Ensure that all applicants are told how LUXOFT GROUP will use CVs and other personal data. **[Russia 5]**

For unsuccessful applicants, explain if you want to keep CVs on file for future use and do not do this if the applicant objects. **[Cyprus 7] [Denmark 14] [France 18] [Malaysia 9] [Poland 6] [Romania 3] [Russia 6] [Sweden 7] [Switzerland 4] [Ukraine 10]**

For successful applicants, be clear what background checks will be made and from whom the information will be sought (e.g. identification checks, certification of right to work, collection of references). Make it clear if the successful completion of background checks is a pre-condition of employment with LUXOFT GROUP. **[Russia 7]**

Refer to the standard notice for applicants at Supplementary Document 1. **[USA 2]**

Employees

Ensure all staff are told how LUXOFT GROUP uses their personal data: relevant information should be included in the Employee Privacy Notice (see Supplementary Document 2).

Where LUXOFT GROUP provides staff data to third parties to provide benefits, make staff aware of this in the literature used to explain the benefits (e.g. pension, insurance or private health providers). If LUXOFT GROUP collects information to pass on to the third parties for administration purposes, do not use this for general employment purposes. **[Malaysia 10] [Vietnam 6]**

DATA QUALITY

General

Only collect information about individuals where there is a clear and foreseeable need for the information. Ensure that when you collect information in application forms/new joiner forms that you identify what information is mandatory or what information is voluntary (i.e by way of a footnote). **[France 11]**

Applicants

If you prepare an application form, only request information which is relevant and not excessive. It should also comply with all relevant anti-discrimination laws. **[France 19]**

Remind interviewers that they should only record information during an interview which is relevant to the recruitment decision: applicants may have a right to see interview notes. **[Cyprus 8]**

RETENTION

General

Carry out file reviews and ensure that irrelevant information is removed and securely destroyed.

Follow the retention guidelines at Supplementary Documents 3.1 and 3.2.

SECURITY

You should ensure that:

- only staff needing access to personnel files to carry out their duties are given such access, and audit trails are put in place to show who has accessed and/or amended such files;
- the taking of employee personal data off-site (e.g. in laptop computers) is controlled and that strict security rules are applied;
- if you are sending confidential or sensitive information about an employee by email or fax, consider whether additional security measures such as encryption are required.

TRANSFERS

[Australia 7] [China 3] [Denmark 11] [India 2, India 6 and India 7] [Malaysia 2 and Malaysia 3] [Russia 3 and Russia 8]

Seek advice from the Data Protection Officer if:

you wish to use a third party outside your own jurisdiction to process employee personal data; or

if you belong to European Operations and

- wish to use a third party outside the EEA or Switzerland or
- have any queries about what data may be transferred to LUXOFT GROUP entities outside the EEA or Switzerland.

RIGHTS

Access

Forward any requests from candidates or employees to see and/or correct their data or to object to the processing of their data to the Data Protection Officer. Remind line managers to do this. **[Australia 9] [Denmark 3] [India 2] [Singapore 7] [Sweden 1]**

Seek the advice of the Data Protection Officer, if needed, in handling subject access requests. **[India 2] [Malaysia 3]**

Marketing

Do not allow third parties to send direct marketing material to employees. **[Cyprus 9] [Malaysia 11]**

Automated decisions

Do not deploy automated decision taking techniques – such as automatic scanning of CVs or absence monitoring systems – without first checking with the Data Protection Officer. On some occasions, specific notices and rights of appeal need to be arranged, and in some countries, the works council may need to be consulted. **[India 3] [China 11] [Malaysia 3] [Netherlands 2]**

SPECIAL SITUATIONS

Requests to disclose data

References: always check with the employee before providing a reference. **[Vietnam 7]**

If asked to disclose information about an employee to a third party, always verify the identity of the third party to check they are entitled to receive the information. Consider whether there is a legal obligation to disclose the information (e.g. in the UK to the Inland Revenue) or whether information is required for legal proceedings or in connection with the prevention or detection of crime. If these considerations do not apply, consider whether it would be fair to the employee to release the information. Please seek further advice from the Data Protection Officer if you are uncertain about the nature of the request. **[Cyprus 10] [India 2 and India 6] [Malaysia 12 and Malaysia 3]**

Where practicable, employees should be told about such disclosures.

Monitoring

The Head of Personnel Department must authorise any requests to monitor specific employees. This would apply to any of monitoring IT Equipment and traffic on the IT Network telephone calls and other forms of monitoring. Before authorising any monitoring, the Head of Personnel Department will: **[Australia 10] [Denmark 15] [France 20] [Malaysia 13] [Switzerland 5] [Vietnam 8]**

- Carry out an impact assessment, to ensure that there is a legitimate purpose for the monitoring, that the impact of the monitoring on the individual is justified and that the intrusiveness of the monitoring is kept to the minimum level necessary to achieve the purpose of the monitoring;

- Consider if employees should be notified that monitoring will be carried out. Where monitoring is used to enforce LUXOFT GROUP rules and policies, the relevant rules and policies and the nature and extent of associated monitoring must be clearly specified. General notice to this effect is included in the Rules on Company information treatment by employees, Information Security Manual and the Employee Privacy Notice; **[China 12] [Cyprus 11] [Luxembourg 6] [USA 2, USA 3]**

- Consider any applicable local law requirements relating to monitoring and interception, particularly as this can constitute a criminal offence in certain countries. In some countries, the works council may also need to be consulted;

- Ensure that the results of employee monitoring will only be available to a limited number of people and may only be used for the purpose for which the monitoring was implemented, unless the results reveal evidence of criminal activity at work, gross misconduct or breaches of health and safety rules which no reasonable employer could ignore; and

- Ensure that emails which are clearly marked as personal will only be read in exceptional circumstances where a problem relating to an employee's excessive or unauthorised use is suspected. You should always contact the appropriate Data Protection Officer and Legal Department before doing so. Note that in some countries, it is prohibited to read any emails marked as private. Please consult the relevant Country Appendices. **Also refer to the local rules for further information. [Australia 10] [Bulgaria 8] [China 12] [Cyprus 12] [Denmark 15] [France 21] [Germany 3] [India 2] [Luxembourg 8] [Mexico 6] [Poland 7]] [Romania 4] [Russia 9] [Sweden 8] [Switzerland 6] [USA 4]**

SUPPLEMENTARY DOCUMENT 1: SAMPLE CONSENT TO THE PROCESSING OF PERSONAL DATA

[Drafted to comply with the UK law only. Amendments might be required to use in other countries]

CONSENT TO THE PROCESSING OF PERSONAL DATA – background check for the purpose of my employment

Purpose of processing

I, _____, hereby authorize **Luxoft UK Limited** (hereinafter – "the Company"), principal place of business: Royal Pavilion, Wellesley Road, Aldershot, GU11 1PZ , United Kingdom, including its affiliated persons, to process my personal data, automatically or otherwise, pursuant to provisions set forth in EU General Data Protection Regulation, and other applicable local laws and as described below, **in order to assist me in finding a job with Luxoft and its affiliates** with an option to save my personal data in the database of the Company and its affiliated persons for a certain period.

List of personal data

I further consent to the processing of the following personal data by the Company, including my (please tick the boxes if you agree):

1. surname 2. first name 3. maiden name 4. date and place of birth 5. e-mail 6. mobile number 7. home number 8. ID number and its details 9. permanent and temporary address	10. prior employment records 11. experience gained from the commencement of working career (Including military service, combined employment, entrepreneurial activity, etc.) 12. job permit/visa/right to work details 13. cause of termination from the last job 14. references from prior employers
15. education(name of the educational institution(s) graduation date line of training or specialty, qualification) 16. postgraduate vocational education (name of the educational or scientific institution, year of graduation)	17. criminal records 18. disqualifications 19. corruption offences 20. debts or any other reason which prevents travelling abroad 21. conflicts of interest with the Company

And any other data set forth in my CV or provided by myself in the course of communication with representatives of the Company; my test/questionnaire survey results (including tests and questionnaires seeking to identify my professional skills, personal and professional qualities and skills, etc.).

Processing activities

The Company is hereby authorized to gather, record, collate, accrue, store update (modify), retrieve, use, make available to the affiliated persons (including distribution, provision, access), depersonalize, block, delete and destroy my personal data within the guidelines as set out by EU General Data Protection Regulation. To the extent permitted by law (e.g. if it is strictly required for the purpose of executing the employment relationship) personal data might be transferred to Luxoft Holding, Inc, its affiliates in the US and other countries, including outside the EU, and will be stored and processed manually and electronically through global systems and tools for internal administrative purposes. Before transfer your personal data to other LUXOFT entities, we take additional security measures to protect your personal data (such as entering into Standard contractual clauses, as prescribed by the EU Commission and LUXOFT Binding Corporate Rules).

I hereby consent to the Company's investigation of the supplied personal data for the purposes mentioned herein by contacting any third parties, whether by way of formal written requests or phone calls.

Also I give my consent that in case of necessity to verify the information regarding existence of a criminal record, the Company may request that I provide an appropriate official document on non-existence (existence) of the criminal record.

Personal data storage term: after the purpose is reached or you restrict/object to the data processing, your personal data will be deleted, unless otherwise prescribed by applicable law. In case your personal data is still necessary we will communicate with you to refresh your consent.

Disclosure to third parties

I hereby acknowledge and understand that for the mentioned purpose the Company may reasonably disclose my personal data to the third parties, including Luxoft background check team, Luxoft trusted external suppliers

to conduct a criminal check in relation to myself, clients who require background check results for their internal compliance, as well as provide any relevant documents containing my personal data.

Hereby I do confirm that any personal data (referrer, prior employers, etc.) of third parties that has been provided by myself has been obtained and provided to the Company legally and with their explicit and freely given consent.

Please note: if during the check we learn any criminal records or any potentially harmful information about you, we will not share this information with a third party or customer.

My confidentiality obligations

I hereby agree to keep confidential any and all data acquired in the course of interaction with the Company, including personal data of the third parties (employees of potential employers, employees of the Company, etc.) I may find out, and further undertake to use any such data exclusively for the purpose of my employment.

Notice about your rights

According to the EU General Data Protection Regulation, you have the right to:

1. access, rectify and erase personal data that relates to you and in line with applicable law 2. to restrict or object the processing of such data 3. as well as the right to data portability	4. right to withdraw this consent without detriment, at any time with future effect 5. right to lodge a complaint with a supervising authority

How to exercise your rights

To rectify or request access to your personal data, withdraw or refuse this consent or execute any other of the aforementioned rights please contact our Data Protection Officer: dpo-uk@luxoft.com at any time. There are exceptions to these rights so that access may be denied, for example, if making the information available would reveal personal information about another person or if Company is legally prevented from disclosing such information.

Right to refuse

I understand that submitting my data and consent is voluntary and that my answers or refusal to provide the answers shall not constitute the reason of refusal of employment. It is possible to withdraw, refuse consent without any detriment.

Questions and concerns

You can contact your local Data Protection Officer by e-mail: dpo-uk@luxoft.com. This consent may be revoked by written notice, e-mailed to: dpo-uk@luxoft.com.

This consent was made in one original provided to the Controller and one copy provided to me.

Surname and initials: _____
Personal signature: _____
Date of consent _____ _____ 20____

SUPPLEMENTARY DOCUMENT 1.1: SAMPLE DATA PROTECTION NOTICE FOR APPLICANTS – ONLINE FORM

Please note that we, the international organization Luxoft Holding, Inc (data controller) will manually and electronically process your personal data such as: your full name and surname, phone number, e-mail address or Skype details, your IT specializations, through our global systems and tools in the amount reasonably necessary for the purposes of managing the recruitment process for a position in Luxoft Holding, Inc or its affiliate or client (the legitimate interest). Your personal data may be accessible to Luxoft Group recruiters outside your own jurisdiction or outside EEA for the purposes above.

We receive your personal data every time when you fill the form on our website, provide us with your CV or other data via e-mail, phone, messenger or by telling it in person. You may contact the Data Protection Officer of controller at GlobalDataProtectionOffice@luxoft.com. The controller will treat your personal data as confidential and will only process such information in compliance with the Luxoft Group Data Protection Policy and applicable legislation.

Your personal data will be kept for unlimited period of time (or until the consent is revoked), unless otherwise prescribed by applicable legal requirements and presuming that it is necessary for the purpose of processing.

You have the right of access and correct, rectify, erase ("right to be forgotten") the collected data, to restrict and object to the data processing, the right to data portability, prevent direct marketing or other types of processing, the right to object to decisions being taken by automated means, lodge a complaint with a supervisory authority.

You may withdraw the consent at any time. If you intend to provide us personal data of another person, please obtain the explicit and freely given consent of this person before such provision. If you do not wish us to use the information which has been provided to us, please e-mail us at GlobalDataProtectionOffice@luxoft.com with the subject heading "Don't use my data" with your name inserted inside.

SUPPLEMENTARY DOCUMENT 2: SAMPLE PRIVACY NOTICE FOR EMPLOYEES
[Drafted to comply with the UK law only. Amendments will be required to use in other countries]

PRIVACY NOTICE FOR EMPLOYEES

LUXOFT UK LIMITED, registered address: Royal Pavilion, Wellesley Road, Aldershot, GU11 1PZ, United Kingdom and Luxoft Holding, Inc., the parent entity of LUXOFT UK LIMITED, and its affiliates ("LUXOFT") are committed to respecting your privacy and applicable privacy laws. We will only process such information as permitted by the EU General Data Protection Regulation and other applicable local laws as described below.

- ***Legitimate interest notice***

LUXOFT has offices across the world, and operating such business involves personal data transfer across offices and countries.

LUXOFT will process your personal data to achieve a legitimate interest, including the following:

recruitment, hiring, employment, payroll, benefits, promotion, performance, management, equality in the workplace, health and safety at work, business travel, protection of an employer's or customer's property, your enjoyment and exercise of your employment rights, ensuring network, information and physical security in LUXOFT offices, transfer of personal data within LUXOFT group for internal administrative purposes, termination of the employment relationship.

	• ***What personal data do we/or we may collect about you?***	• ***What is the purpose of the processing?***
	General personal information: your name, home address, postal address, temporary address, phone numbers (home and mobile), personal email, citizenship, immigration status, age, date of birth, family status, passport and ID number, residence permit, work permit, written and electronic communications via corporate email.	The processing of this personal data is necessary to identify you as an employee and to comply with the employer's legal obligations: to establish and perform the employment contract, to maintain or terminate the employment relationship and to enable you to perform your job, to manage data transfers between different subsidiaries and branches. We may use your corporate email, name, position and location to inform you about corporate news, events, policies, trainings and to address you other internal communications important for the performance of your work duties.
	Identifying information: your photo image, personal identification number and your corporate system account.	The processing of this personal data is necessary to identify you in the internal corporate systems, to provide access to LUXOFT' s offices, management of LUXOFT's IT systems and infrastructure, inclusion in company directories and provision of communication services such as e-mail, telephone and internet access. Please note, that you may choose the way how we use your photo or you may object to processing of your photo.
	Insurance information: your national insurance details, medical insurance details, beneficiaries' details in relation to life insurance or other benefits, emergency contacts, family status, information about family members (full name, date of birth, insurance number gender and national personal ID number), data on alimony payments and other contributions.	The processing of this personal data might be necessary for the provision of medical insurance to you and your beneficiaries, for applicable benefits, alimony payments, guarantees or relocation assistance, occupational health, retirement plans.
	Your skills: information concerning your employment history, profession, education and skills, including: job title, previous employers, division, position, business unit, location of working place, your business contacts, referees and their contacts, professional experience, education, performance history, billing time, training records.	The processing of this personal data is necessary for recruitment, hiring and internal mobility process. Your billing time/time sheet may be available to the respective client as a part of invoice. In specific cases, and only upon the client's request, we may show your CV to a potential client for business engagement or to current client to confirm the high level of skills of our members of staff providing the services. Such proof of quality is a key to our and our client's businesses. The CV will only contain your name, date of birth, education

		history, employment history, degrees, certifications and professional skills (if any). In any event, the potential / current client is under the obligation to delete your CV immediately after the quality of our services has been confirmed.
	Payroll data: the amount of your salary, bonuses, remuneration, social and other benefits, KPI goals and results, offer details, bank details, tax number.	The processing of this personal data is necessary to comply with the employer's obligations: payroll, benefits, compensation and quota commission, succession management, award recognition, audits
	Security data: CCTV records, entrance-exit time in the office, office entrance records, logs of your access and actions in the corporate internal systems, IP of your personal device (if is used for access to LUXOFT network).	The processing of this personal data is necessary to monitor your working time, protect the security of LUXOFT's premises, assets, systems, and intellectual property and enforcing company policies, including monitoring communications where permitted by local law and in accordance with LUXOFT's Regulations on the processing of Personal Data, Rules on Company Information Treatment by Employees, Information Security Manual, Instruction on use of corporate email Use of Corporate Electronic Mail and for investigations and disciplinary actions.
	Travel-related data: your trip itineraries with dates and times, visa, driving licence details, current address, expense records such as: details of out of pocket expenses, corporate credit cards, company cars or private cars where an allowance is claimed and mobile phone costs.	The processing of this personal data is necessary to comply with the employer's obligations to manage relocation, business travels, expenses and compensations.
	Performance data: your training/testing/assessment/appraisal/survey results, risk and value assessment, information concerning your performance, career plans, conducts.	The processing of this personal data is necessary for your performance management, training and professional development. The surveys is a mood monitoring tool, which helps us to protect you and ensure your comfortable communications,
	Sensitive data: where permitted by local law and upon your explicit consent: background checks, which include information about violation of laws or breach of company policies, where permissible.	The processing of this personal data is necessary to comply with applicable laws and protection of LUXOFT's legitimate business interests and legal rights, including, but not limited to, performance of LUXOFT contractual obligations, to evaluate eligibility for employment and applicable benefits, to use in connection with legal claims, compliance, regulatory, investigative and disciplinary purposes (including disclosure of such information to authorities)
	Other employment data: your vacations, medical leave information, sickness and accident records, medical certificates, workplace adjustments, other documents required to confer special benefit status, such as information concerning pregnancy status and age of children if applicable.	The processing of this personal data is necessary to comply with the employer's obligations: vacations and sick leaves management, payroll and compensations.
	Your **conflicts of interests** with LUXOFT.	The processing of this personal data is necessary to comply with the employer's Code of conduct and Conflict of interest policy.
	Data on your **shareholding** in LUXOFT.	The processing of this personal data is necessary to manage your stock plan (in case you have LUXOFT shares).

- ***Retention period***

- LUXOFT will keep this information, together with data retained from the application and selection process, for the course of the employment relationship and, to the extent permitted for legal, social security or /Tax reasons.
- Your personal data that we process for any purpose or purposes shall not be kept for longer than it is necessary for that purpose or those purposes. This time may vary depending on the type of the processed personal data and the

purposes of processing. Notwithstanding these provisions, we will retain your personal data to the extent that we are required to do so by law.

- For more information on what data we need to keep and for how long post termination of employment, please contact the Data Protection Officer (see below).

- ***Transfer of your personal data***

- To the extent permitted by law (e.g. if it is strictly required for the purpose of executing the employment relationship) personal data might be transferred to Luxoft Holding, Inc, its affiliates in the US and other countries, including outside the EU, and will be stored and processed manually and electronically through global systems and tools for internal administrative purposes. Before transfer your personal data to other LUXOFT entities, we take additional security measures to protect your personal data (such as entering into Standard contractual clauses, as prescribed by the EU Commission and LUXOFT Binding Corporate Rules).
- Access to personal data is limited and will only be allowed on a strict need to know basis. Your personal data will primarily be processed by employees of the HR, IT and finance, legal and facilities departments, where relevant and necessary. We have taken steps to ensure that there is adequate protection for your personal data in these circumstances.
- Personal data may be shared with government authorities and/or law enforcement officials if required for the purposes above, if mandated by law and if required for the legal protection of LUXOFT's legitimate interests in compliance with applicable laws.
- Personal data may also be shared with third party service providers, who will process it on behalf of LUXOFT for the purposes above. Here and below, references are given to the alphabetical items in the left column of the table above, such third parties include, but are not limited to, payroll service providers (e, travel agencies and travel service providers (g), relocation service providers (g), banks (e), credit card companies (e), brokers (l), medical services and medical insurance providers (c), training providers (h), survey service providers (h), testing/assessment/appraisal service providers (h), internal communication tools (a, d), investigators (k), employee hotline administrators (k), data custodians (a), current and potential clients (b, d), auditors (b, e), external consultants (b, e), IT and telecommunication operators (f), landlords and other physical security service providers (f), other external service providers, etc. Before transfer your personal data to third parties, we take additional security measures to protect your personal data (such as entering into data protection agreements or special amendments to our contracts).
- In the event that the business is sold or integrated with another business, your details may be disclosed to our advisers strictly on a need to know basis and any prospective purchaser's adviser and will be passed to the new owners of the business.

- ***Security measures***

- LUXOFT has taken appropriate technical, administrative, physical and procedural security measures, consistent with local and international information practices, to protect the personal data from misuse, unauthorized access or disclosure, loss, alteration, or destruction. These measures include:

  - *Physical safeguards*, such as locked doors and file cabinets, controlled access to our facilities, and secure destruction of media containing personal data.
  - *Technology safeguards*, such as use of anti-virus and endpoint protection software, passwords.
  - *Organizational safeguards*, through training and awareness programs on security and privacy, to ensure employees understand the importance and means by which they must protect personal data, as well as through privacy policies and policy standards that govern how LUXOFT treats personal data.

- LUXOFT will process your personal data primarily on the basis of, Art. 6 para. 1 lit. b) and Art. 6 para. 1 lit. f) of the EU General Data Protection Regulation. In exceptional cases, LUXOFT may also process your personal data on the basis of Art. 6 para. 1 lit. a), and lit. c) to e) of the EU General Data Protection Regulation. In case of the processing of sensitive data in terms of Art. 9 para. 1 of the EU General Data Protection Regulation (e.g. health data), LUXOFT will process this information on the basis of Art. 9 para. 2 EU General Data Protection Regulation https://gdpr-info.eu/.

- ***Your rights***

- According to the EU General Data Protection Regulation, you have the right to access, rectify and erase personal data that relates to you and in line with applicable law, to restrict or object the processing of such data. You also have the right to lodge a complaint with a supervising authority. To rectify or request access to your personal data or execute any other of the aforementioned rights please contact your Data Protection Officer at any time. There are exceptions to these rights so that access may be denied, for example, if making the information available would reveal personal information about another person or if LUXOFT is legally prevented from disclosing such information
- For questions and concerns you can also contact the Data Protection Officer, LUXOFT UK LIMITED, 44 Featherstone Street, London, EC1Y 8RN, e-mail: dpo-uk@luxoft.com.

- ***Your obligations***

- If you intend to provide us personal data of another person (e.g. emergency contacts, beneficiaries, for insurance, relocation, conflict of interest, referral, etc.), please obtain the explicit and freely given consent of this person before such provision and to its processing.
- It is important that we maintain up to date records of key information on you. Please notify your HR representative of any changes in your personal circumstances as soon as they occur (e.g. change of address, marital status, and emergency contacts). From time to time we may ask you to complete a new personal information form to ensure our records are up to date.
- Where we require personal data to comply with legal or contractual obligations, then provision of such data is mandatory: if such data is not provided, then we will not be able to manage the employment relationship, or to meet obligations placed on us. In all other cases, provision of requested personal data is optional.

I hereby confirm that I have read and become familiar with the order of processing of my personal data and I have been notified of my privacy rights.

Signature: _____

Full Name:_____

Date:_____

Consent to use of photo

Please confirm by ticking the boxes below if you agree to your photo being used for the following purposes:

[ ] corporate directory (which all employees of LUXOFT have access to);

[ ] internal corporate correspondence;

[ ] internal communications and newsletters (to be sent to all employees of LUXOFT);

[ ] external news and media (including online media) in connection with events and updates about LUXOFT.

Please note that this is consent according to applicable data protection law in order for LUXOFT to use your photo as described herein. You have the right to withdraw your consent at any time with future effect.

Your consent is entirely voluntary and you will not be subject to any disciplinary action if you chose not to grant your consent. However if you refuse your consent, it can happen that you will not be considered in internal and external publications, as the lack of a picture could be an issue with regards to the corporate identity.

Your photo will be accessed through the software used for the corporate directory, corporate mail; furthermore for internal and external publications, worldwide marketing functions will access the photo in the corporate directory. With regards to sales employees, we deem external publication of your picture and name and professional contact information to be justified in line with your role.

Please be assured that your personal data is stored secure and safe and utilised fairly in compliance with the principles of proportionality and adequacy in particular and in general with the EU General Data Protection Regulation. Access to your data is strictly limited on a need-to-know basis. The LUXOFT data protection officer monitors the proper handling of your data.

Signature: _____

Full Name:_____

Date:_____

SUPPLEMENTARY DOCUMENT 3.1: GENERAL RECORDS RETENTION PERIODS FOR INTERCOMPANY DATABASES

Below are the general retention periods applicable to intercompany databases, containing the personal data originated from different locations and when it is not possible to determine and implement the local retention periods (Supplementary document 3.2) applicable to each part of personal data. After the expiration of the period, the data must be securely deleted, unless data subject provided the consent for longer retention period.

1.	Unsolicited application forms/CVs (not to be pursued)	No longer than two (2) months
2.	Application Forms/CVs	No longer than two (2) months
3.	Interview notes	No longer than two (2) months
4.	References given to a potential future employer	Six (6) months from the date of issue.
5.	Absence records	Three (3) years from termination of employment.
6.	Appraisals and performance reviews	Six (6) months from termination of employment.
7.	Records relating to promotion	Six (6) months from termination of employment.
8.	Reference provided by a former employer	Six (6) months from receipt.
9.	Summary of record of service	One (1) year from termination of employment (unless the employee has agreed details should be kept longer).
10.	Payroll and tax records	Six (6) to ten (10) years depending on the type of record.
11.	Records relating to accident or injury at work	Three and a half (3.5) - Six (6) years from date of incident dependant on type of record
12.	"Spent" disciplinary proceedings Warnings	Twelve (12) months
13.	Complaints	Six (6) months after resolution of the complaint
14.	Criminal Conviction	Upon first annual update after such convictions becoming "spent"
15.	Ex-Employees records	Archived for six (6) years and then securely destroyed.
16.	Clients	Three years
17.	Prospects	Within 1-2 years after consent was collected
18.	Contractors	3-4 years

SUPPLEMENTARY DOCUMENT 3.2: HR RECORDS RETENTION PERIODS FOR LOCATIONS

Unless otherwise specified below or unless there is a reasonable belief that legal proceedings will be started, all documents should be destroyed at the end of the retention period. If it is likely that legal proceedings will start, then records should be retained and passed to the Legal Department. Any queries regarding retention periods should be referred to the Data Protection Officer. See Country Appendices for more detail.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
Unsolicited application forms/ CVs (not to be pursued)	Unsolicited information may only be retained if it is reasonably necessary for the organisation's functions or activities. Once such information is no longer needed, it should be destroyed or de-identified.	No statutory retention period so UK position likely to be acceptable.	The law does not determine specific retention period. For a period that does not exceed the time necessary for the purposes for which such data are being processed; personal data which are to be retained for a longer period of time for statistical purposes shall be stored in a format precluding the identification of individuals. For applicants who are approved on the basis of such CVs, the data may become part of the employee's personal file and to be kept during the employment period. After the termination of the employment contract the CVs should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which the CVs have been collected/ stored. The employees may grant their consent for a specific term for which their CVs could be kept after the termination of the employment contract depending on the purposes for the CVs may be processed.	No statutory retention period so UK position likely to be acceptable.	Consent of applicant is required to use application forms / CVS for future use if applicant is unsuccessful. If consent is not obtained application forms / CVs may be used only until employee selection period ends. If a candidate expressly requests deletion of their data, this should be done immediately. No statutory retention period.	Permanently	No statutory retention period. The Danish Data Protection Agency prescribes that applicant data should be deleted as soon as possible after the applicant has been informed that he/she has been rejected. Generally the data should be kept for no longer than six (6) months. Consent of applicant is required to use application forms/CVs for future use if applicant is rejected. If consent is not obtained, application forms/CVs may be used only until employee selection period ends. If a candidate expressly requests deletion of its data, this should be done immediately.	Applicant data should generally be kept for no longer than two (2) months after an applicant has been informed that they have been rejected. If a candidate expressly requests deletion of their data, this should be done immediately. If the data shall be kept for the above retention period, in this case the data has to be blocked (Sperrung, Section 35 para 3 German Data Protection Act) in order to respect the deletion request.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) considers that the retention of such data should not exceed two (2) years as from the last contact with the applicant. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after two (2) years.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. The Malaysian data protection authority has issued a guideline that personal data collection forms used in commercial transactions must be disposed within a period not exceeding fourteen (14) days except if/ unless the forms carry legal values in relation to the commercial transaction. It is also recommended that consent of the applicant is required to use application forms/ CVs for future use. This applies to unsuccessful applicants and unsolicited applications not to be pursued. If the applicant expressly requests deletion of its personal data, this should be done immediately.	According to Articles 516 and 804 of the Federal Labour Law ("FLL") it is not necessary to hold files for more than a year. Thus, our recommendation is to keep them in archives for one (1) year.	No statutory retention period. The general rule applies: such data should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail. Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant.
Application Forms/ CVs	Once such information is no longer needed, it should be destroyed or de-identified. For employees, it would form part of an employee record, which for the purposes of the Fair Work Act 2009 must be retained for 7 years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	The law does not determine a specific retention period. The CVs could be kept in a form which permits identification of the applicants for no longer than it is necessary for the purposes for which the CVs were collected or for which they are further processed. For unsuccessful candidates the CVs could be processed till the end of the respective recruitment process. For being keep and to use for further recruitment procedures, the consent of the candidates is needed or at least they should be aware that their CVs will be used in such a way and should be able to object at any time. For successful candidates the data could become part of the employee's personal file and to be kept during the employment period. After the termination of the employment contract the CVs should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which the CVs have been collected/ stored. The employees may consent their CVs to be kept for a specific term after the termination of the employment contract depending on the purposes for which the CVs may be processed. (Recommended term in such case – up to five (5) years after the termination of the employment contract (this is the longest period of prescription))	No statutory retention period so UK position likely to be acceptable.	Consent of applicant is required to use application forms / CVS for future use if applicant is unsuccessful. If consent is not obtained application forms / CVs may be used only until employee selection period ends. If a candidate expressly requests deletion of their data, this should be done immediately. No statutory retention period.	Permanently	No statutory retention period. Consent of applicant is required to use application forms/CVs for future use if applicant is rejected. If consent is not obtained, application forms/CVs may be used only until employee selection period ends or until five (5) years after the termination of employment.	Applicant data should generally be kept for no longer than two (2) months after an applicant has been informed that they have been rejected. If a candidate expressly requests deletion of their data, this should be done immediately. If the data shall be kept for the above retention period, the data has to be blocked (cf. above).	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. The Malaysian data protection authority has issued a guideline stating that personal data collection forms used in commercial transactions must be disposed within a period not exceeding fourteen (14) days except if/ unless the forms carry legal values in relation to the commercial transaction. For successful applicants, the application forms/ CVs could become part of the employee's personal file to be kept during the employment period if consent is obtained.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	No statutory retention period. The general rule applies: such data should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail. Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant. If the applicant becomes an employee, such data may become part of the employment record, if necessary (i.e. the employer has a good reason to keep such records). Employee records must be kept for seven (7) years after the termination of employment.
Interview notes	Once such information is no	No statutory retention period so	No statutory retention period so UK position likely	No statutory retention period so UK position likely	No statutory retention period. If a candidate expressly requests	Permanently	No statutory retention period. The Danish Data Protection Agency prescribes that applicant data/interview notes should be	Applicant data should generally be kept for no longer than two (2)	No statutory retention period. However, in the event the document contains sensitive personal data or information	For rejected applicants / unsolicited applications not pursued, please refer to the retention period in the first row	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the	Although according to Articles 516 and 804 of the FLL it is	No statutory retention period. The general rule applies: such data

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
	longer needed, it should be destroyed or de-identified. For employees, it would form part of an employee record, which for the purposes of the Fair Work Act 2009 must be retained for seven (7) years after the termination of employment.	UK position likely to be acceptable.		to be acceptable.	deletion of their data, this should be done immediately. Candidate has a right of access to interview notes.		deleted as soon as possible after the applicant has been informed that he/she has been rejected. Generally the data should be kept for no longer than six (6) months. Consent of applicant is required to use application data/interview notes for future use if applicant is rejected. If consent is not obtained, application data/interview notes may be used only until employee selection period ends or until five (5) years after the termination of employment.	months after an applicant has been informed that they have been rejected. If a candidate expressly requests deletion of their data, this should be done immediately. If the data shall be kept for the above retention period, the data has to be blocked (cf. above).	pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	of this table. For successful applicants, please refer to the retention period in the second row of this table.	fulfilment of the purpose for which the data was collected. For unsuccessful applicants and unsolicited applications not to be pursued, kindly refer to the first row of this table. For successful applicants, kindly refer to the second row of this table.	not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail. Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant. If the applicant becomes an employee, such data may become part of the employment record, if necessary (i.e. the employer has a good reason to keep such records). Employee records must be kept for seven (7) years after the termination of employment.
References given to a potential future employer	Information should be destroyed or de-identified after it is no longer required.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	No statutory retention period so UK position likely to be acceptable.
Absence records showing incidence of sickness absence, annual leave and other approved and unapproved absence	Employee records must be kept for seven (7) years after the termination of employment.	Employee records should be kept at an address in the BVI for not less than six (6) years from the termination of employment.	Fifty (50) years when information is transferred to the employees' pay-roll sheets or becomes part of orders for non-paid leave for more than thirty (30) days. After expiry of the 50-year term, do not destroy these documents and/or data before prior confirmation from the Legal Department.	Three (3) years from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years. Such information includes details of holidays, annual and sick leave with pay granted during each wage period.	According to Article 804 of the FLL, attendance records should be kept in files during the last year of the employment relationship and one year after termination. Thus, our suggestion is to hold them in files for five (5) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. Examples are records on medical/physical incidents which may only become apparent after 30 years. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
													Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Appraisals and performance reviews	Employee records must be kept for seven (7) years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	The law does not determine a specific retention period. These data should be kept in a form which permits identification of the employees for no longer than it is necessary for the purposes for which they were collected or for which they are further processed. Such data are part of the employee's personal file and could be kept during the employment period. After the termination of the employment contract these data should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which they have been collected/ stored. The employees may consent to a specific term for which these data to be kept after the termination of the employment contract depending on the purposes for which they may be processed. (Recommended term in such case – up to five (5) years after the termination of the employment contract (this is the longest period of prescription)).	Three (3) years from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Records relating to promotion	Employee records must be kept for seven (7) years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	Fifty (50) years from termination of employment, when information was transferred to the employees' pay-roll sheets, employment contract, orders for reappointment and other similar. After expiry of the 50-year term, do not destroy these documents and/or data before prior confirmation from the Legal Department. For other details related to the promotion the law does not determine specific retention period. These data should be kept in a form which permits identification of the data subjects for no longer than it is necessary for the purposes for which they were collected or for which they are further processed. Such data could be part of the employee's personal file and could be kept during the employment period. After the termination of the employment contract these data should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which they have been collected/ stored. Since there is no statutory retention period UK position likely to be acceptable. The employees may consent to a specific term for which these data to be kept after the termination of the employment contract depending on the purposes for which they may be processed. (Recommended term in such case – up to five (5) years after the termination of the employment contract (this is the longest period of prescription)).	Three (3) years from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years. Such information includes those concerning occupation or appointment.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Refere	If it	No	The law does not determine specific	No statutory	No statutory	Perma	No statutory retention period.	No statutory	No statutory retention period.	For rejected applicants /	No statutory retention period.	Although	No statutory

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
nce provided by a former employer	becomes part of an employee record, it should be kept for seven (7) years after the termination of employment.	statutory retention period so UK position likely to be acceptable.	retention period. These data could be kept in a form which permits identification of the data subjects for no longer than it is necessary for the purposes for which they were collected or for which they are further processed. Such data could be are part of the employee's personal file and could be kept during the employment period. After the termination of the employment contract these data should be destroyed within reasonable time, unless their storage is still necessary for the purposes for which they have been collected/ stored. The employees may consent these data to be kept for a specific term after the termination of the employment contract depending on the purposes for which they may be processed. (Recommended term in such case – up to 5 years after the termination of the employment contract (this is the longest period of prescription)).	retention period so UK position likely to be acceptable.	retention period so UK position likely to be acceptable.	nently	Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment.	retention period so UK position likely to be acceptable.	However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	unsolicited applications not pursued, please refer to the retention period in the first row of this table. For successful applicants, please refer to the retention period in the second row of this table.	The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. For unsuccessful applicants and unsolicited applications not to be pursued, kindly refer to the first row of this table. For successful applicants, kindly refer to the second row of this table.	according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	retention period. The general rule applies: such data should be deleted as long as it is no longer necessary. The longer such data is kept, the harder it will be to justify such retention as the rights of the individual will prevail. Best practice based on an Exemption Decree is four (4) weeks after the end of the application, or one (1) year with consent of the applicant. If the applicant becomes an employee, such data may become part of the employment record, if necessary (i.e. the employer has a good reason to keep such records). Employee records must be kept for seven (7) years after the termination of employment.
Summary of record of service (including name, position held and dates of employment)	Employee records should be kept for seven (7) years after the termination of employment.	Employee records should be kept at an address in the BVI for not less than six (6) years from the termination of employment.	Fifty (50) years from termination of employment.	Three (3) years from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment.	No statutory retention period with exemption of (i) consent to overtime work according to working time law (ii) maternity protection law; respectively two (2) years retention. For the rest UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years. Such information includes name, occupation or appointment and date of commencing and leaving employment.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Payroll and tax records	Employee records should be kept for seven (7) years after the termination of employment.	Records and underlying documentation are to be retained for a minimum of five (5) years.	Payroll - fifty (50) years from making the files After expiry of the 50-year term, do not destroy these documents and/or data before prior confirmation from the Legal Department. Tax records – ten (10) years from the end of the tax year in which the tax obligation arose.	Seven (7) years.	Six (6) years after the end of the year to which they refer.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	Six (6) to ten (10) years depending on the type of record.	Payroll Information: shall be maintained for a period of three (3) years after the date of the last entry made therein. Taxation Records: assessees are required to preserve the books of account for a period of seven (7) years from the end of the relevant financial year to which such records pertain to.	Ten (10) years (minimum) from the date of creation of the document concerned.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years. Such information includes wage rates.	According to Article 804 of the FLL, evidence of payment of profit sharing, vacation, Christmas bonus, premiums, as well as any social security payments, contributions and quotas should be kept in files during the last year of the employment	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
												relationship and one (1) year after termination. Thus, our suggestion is to hold them in files for five (5) years. Regarding tax records, our recommendation is to keep them for ten (10) years.	individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Records relating to accident or injury at work	Where the accident or injury is a notifiable incident, records must be kept for at least five (5) years.	No statutory retention period so UK position likely to be acceptable.	Fifty (50) years from termination of employment. After expiry of the 50-year term, do not destroy these documents and/or data before prior confirmation from the Legal Department.	Three (3) years from termination of employment.	No statutory retention period so UK position likely to be acceptable. [Cyprus 4]	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	No statutory retention period so UK position likely to be acceptable. Note: There are health and safety law retention periods which mainly relate to operations and are not considered herein.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. However, in accordance with the legal limitation period, it is recommended to keep such data for at least ten (10) years from termination of employment.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of all records of contributions payment made to the Social Security Organization for seven (7) years.	Although Article 297 of the Social Security Law (SSL) establishes a statute of limitations of 5 years, , our recommendation is to keep them in archives for ten (10) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. Examples are records on medical/physical incidents which may only become apparent after 30 years. The prolonged retention needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
"Spent" disciplinary proceedings Warnings	Employee records should be kept for seven (7) years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	After one (1) year of impeccable work. Disciplinary sanctions other than dismissal may be stricken by the employer before the lapse of the time limit of 1 year, if the employee has not committed other breaches of work discipline.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently; warnings may be kept for 30 years only	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. This however needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Grievances	Employee records should be kept for seven (7) years after the	No statutory retention period so UK position likely to be acceptable.	No statutory retention period, so same as UK.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee	No statutory retention period so UK position likely to be acceptable.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
	termination of employment.						records may be kept until five (5) years after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.		corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract.		recommendation is to keep them in archives for five (5) years.	the interest of the company. This however needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Criminal Convictions	If provided by an employee and form part of an employee record, then seven (7) years after the termination of employment.	No statutory retention period so UK position likely to be acceptable.	If a candidate provides information that he has a criminal record, this record should be deleted once the information has been verified unless the information is clearly relevant to the ongoing employment relationship.	No statutory retention period so UK position likely to be acceptable.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected.	Same as UK.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	Data related to criminal convictions may not be kept for longer than two (2) years.	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected.	Although Articles 516 and 804 of the FLL establish that it is not necessary to hold files for more than a year, considering the statute of limitations provided by Article 104 of the Federal Criminal Code (FCC), our recommendation is to keep them in archives for ten (10) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. This however needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.
Ex-Employees records	Seven (7) years after the termination of employment.	Employee records should be kept at an address in the BVI for not less than six (6) years from the termination of employment.	Fifty (50) years from termination of employment for pay-rolls and documents related to the length of service and social insurance term, including employment contract, work-books (not received by the employee), journals, certificates, orders for appointment, reappointment, termination and long-term non-paid leave (more than thirty (30) days) and other similar documents that can serve as a basis for pension. For other data/records/documents related to ex-employees the retention periods mentioned above should be also applicable. After expiry of the 50-year term, do not destroy these documents and/or data before prior confirmation from the Legal Department.	Three (3) years from termination of employment.	No statutory retention period so UK position likely to be acceptable.	Permanently	No statutory retention period. Such data should not be retained for longer than is necessary for the purposes for which the data was collected. The Danish Data Protection Agency prescribes that employee records may be kept until five (5) years after the termination of employment. Such data can be kept longer if needed in order to e.g. comply with legal obligations or to defend or pursue a legal claim.	No statutory retention period so UK position likely to be acceptable (with exemption of the tax and social security records, cf. above). It is recommended to retain the complete personnel file for the applicable contractual forfeiture period or three years commencing from the end of the year when the employment has terminated (statutory limitation period for civil law claims). At least in case the employee requests deletion, one should consider blocking (Sperrung) according to Section 35 para 3 German Data Protection Act.	No statutory retention period. However, in the event the document contains sensitive personal data or information pertaining to the candidate(s), the law mandates that a body corporate or a person on its behalf shall not retain such information for longer than it is required for the purposes for which the information may be lawfully used (the information collected shall be used for the purpose for which it has been collected) or the same is otherwise required under any law for the time being in force.	No statutory retention period. The default position applies: such data should not be retained for longer than is necessary for the purposes for which the data was collected. Please note that the French data protection authority (CNIL) has issued a recommendation not to retain such data for longer than the duration of employment. In practice, the Luxembourg data protection authority frequently adheres to the recommendations made by the CNIL. It is therefore recommended to destroy such data after termination of the employment contract, with the exception of data governed by specific rules (e.g. employment contract – ten (10) years; accounting documents related to duration of employment – three (3) years; please also refer to the specific rules in the rows above).	No statutory retention period. The general rule is that such data should not be retained for longer than is necessary for the fulfilment of the purpose for which the data was collected. Malaysian law requires employers to keep information registers of their employees for not less than six (6) years.	Although according to Articles 516 and 804 of the FLL it is not necessary to hold files for more than a year, our recommendation is to keep them in archives for five (5) years.	Employee records must be kept for seven (7) years after the termination of employment. They may be kept longer if necessary in the interest of the company. This however needs to be duly substantiated and documented, also in light of the rights to privacy such individual has. Please note that there is a legal tension between the Dutch data protection rules (delete as soon as possible) and the need for such data for evidence in employment proceedings.

Document	Australia	British Virgin Islands (BVI)	Bulgaria	Canada	Cyprus	China	Denmark	Germany	India	Luxembourg	Malaysia	Mexico	Netherlands
								Documents relating to company pension grant should be retained until due date (retirement of employee).					

Document	Poland	Romania	Russia	Singapore	Sweden	Switzerland	UK	Ukraine	USA[4] [USA 5]	Vietnam	Korea
Unsolicited application forms/CVs (not to be pursued)	If the application was made without the particular recruitment process, then the candidate should be asked whether the CV can be kept for particular period of time (e.g. two (2) months) for new openings, otherwise it should be deleted. Unless the recruitment process will be initiate during agreed period of time, the application should be deleted. After completion of the recruitment process application should be deleted.	No statutory retention period.	Russian legislation doesn't contain definition of "unsolicited application forms/CVs". There are only restrictions according to personal data legislation: a candidate grants consent for personal data processing which is effective till its revocation by a candidate, but no less than Fifty (50) years.	No statutory retention period. Under the Singapore Personal Data Protection Act 2012 ("PDPA"), an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than six (6) months unless necessary for legal or business purposes.	No statutory retention period. Personal data regarding rejected candidates must be deleted as soon as the information is no longer needed for the purpose for which the information was collected, i.e. when the recruitment process has been concluded (unless the candidate has consented that the information may be kept on file). However, in case of a possible dispute (e.g. on grounds of discrimination) the data may be stored for a period of two (2) years or if such dispute is initiated until the dispute is finally settled.	Documents to be returned to the applicant as soon as not necessary anymore (After three months at the latest documents should be deleted to follow the practice of the Government). If a candidate expressly requests deletion of their data, this should be done immediately.	Nine (9) months from date of receipt (unless candidate has agreed details should be kept on file or requested removal). (Recommended period based on the fact that under the new employment tribunal process, it could take some time for the claim to be processed and so employers may not be made aware of the claims for much longer than it took previously).	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives, which is one (1) year for the documents of candidates not accepted for employment.	FED: One (1) to two (2) years (depending on statute) from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. CA: Two (2) years from date the records are created or received. If complaint is filed by applicant, then records must be kept until final disposition. NY: Three (3) years from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. TX: One (1) year following receipt. MI/WA: No regulations so follow FED.	No statutory retention period. However, as the document arguably might contain personal information of the candidate/employee, privacy law suggests that those who collect or process such personal information may store it only for a period as agreed by the candidate/employee.	
Application Forms/CVs	The candidate's data should be kept as long it is necessary for particular requirement process. After completion of the recruitment process application should be deleted.	Thirty (30) years from the hiring date.	Russian legislation doesn't contain definition of "application forms/CVs". If application forms/CVs are taken from public source (Internet, social networks) – no need in candidates consent for personal data processing, but no less than fifty (50) years.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than six (6) months unless necessary for legal or business purposes.	No statutory retention period. In general such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded. If kept in the employees' personal files it may be kept at least until the termination of the employment. Please note that the retention period after the termination of the employment shall in no case be shorter than applicable statutory minimum retention periods (e.g. personal data processed for accounting purposes shall be stored for seven (7) years according to the requirements in the Swedish Accounting Act). Please note that the Swedish Data Protection Authority has provided recommended retention periods during which personal data may be stored. In general employee personal data should be deleted once the employment relationship has ended. However, data may be stored for as long as (i) there is a potential for a dispute between the company and the former employee, or (ii) the information is necessary with regard to administrative purposes e.g. to administer pension payments, issue work certificates or to provide references to other employers. In addition, the company may keep factual information for a longer period (as long as the information is still relevant) such as "termination due to redundancy", "dismissal" or "termination for personal reasons"- notes or likewise together with copies of letters of recommendation	No statutory retention period. Documents to be returned to the applicant as soon as the application process is over. (After three months at the latest documents shall be deleted to follow the practice of the Government). If a candidate expressly requests deletion of their data, this should be done immediately.	Nine (9) months after completion of the recruitment exercise to which they relate (unless the applicant has issued a complaint about the application process or decision). (Recommended period based on the fact that under the new employment tribunal process, it could take some time for the claim to be processed and so employers may not be made aware of the claims for much longer than it took previously). Information relating to successful candidates may, where relevant, be transferred to the employees' personnel file	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	FED: One (1) to two (2) years (depending on statute) from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. CA: Two (2) years from date the records are created or received. If complaint is filed by applicant, then records must be kept until final disposition. NY: Three (3) years from date hiring process is completed or, if hired, no less than three (3) years after termination of employment. If complaint is filed by applicant, then records must be kept until final disposition. TX: One (1) year following receipt. WA/MI: No regulations so follow FED.	Same as above.	

[4] Retention of HR records in the United States is governed by both federal (FED) and state law. Luxoft offices located in different states, and they may have different statutory requirements as indicated in this matrix. If the state and federal retention periods differ, employer must comply with the jurisdiction that requires the longest retention period. If your location has less than 50 employees, then Family Medical Leave Act (FMLA) does not apply, but other FED statutes may still be applicable. Due to its strict standards FMLA may nevertheless serve as a best practice in these cases. This matrix does not include local city ordinances that may apply.

Document	Poland	Romania	Russia	Singapore	Sweden	Switzerland	UK	Ukraine	USA[4] [USA 5]	Vietnam	Korea
					or grades provided to the employee e.g. for evaluation of re-employment rights.						
Interview notes	The candidate's data should be kept as long it is necessary for particular requirement process. After completion of the recruitment process application should be deleted.	No statutory retention period.	Russian legislation doesn't contain definition of "interview notes".	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than six (6) months unless necessary for legal or business purposes.	Please see comment on Application Forms/CVs above.	No statutory retention period. Documents to be deleted as soon as the application process is over. (After three months at the latest documents shall be deleted to follow the practice of the Government), If a candidate expressly requests deletion of their data, this should be done immediately.	Nine (9) months after the interview (either internal or external) (unless the candidate has made a complaint about the interview). (Recommended period based on the fact that under the new employment tribunal process, it could take some time for the claim to be processed and so employers may not be made aware of the claims for much longer than it took previously).	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	FED: One (1) to two (2) years (depending on statute) from date hiring process is completed. If complaint is filed by applicant, then records must be kept until final disposition. CA: Two (2) years from date the records are created or received. If complaint is filed by applicant, then records must be kept until final disposition. NY: Three (3) years from date hiring process is completed or, if hired, no less than three (3) years after termination of employment. If complaint is filed by applicant, then records must be kept until final disposition. TX: One (1) year following receipt. MI/WA: No regulations so follow FED.	Same as above.	
References given to a potential future employer	From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination but only when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)	No statutory retention period.	Russian legislation doesn't contain definition of "references given to a potential future employer".	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than six (6) months unless necessary for legal or business purposes.	Please see comment on Application Forms/CVs above.	No statutory retention period so UK position likely to be acceptable.	Six (6) months from the date of issue of reference.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	No per se statutory retention period so comply with UK standard.	Same as above.	
Absence records showing incidence of sickness absence, annual leave and other approved and unapproved absence	From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination of the employment but only when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)	Thirty (30) years from the inception date of the documents.	Absence records showing incidence of sickness absence, annual leave – five (5) years. Long-term absence (including business trips, maternity leave, unpaid vacation etc.) – fifty (50) years.	No statutory retention period. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained ten (10) years from termination of employment.	Three (3) years from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, medical records and other documents of secondary importance are kept three (3) years from termination of employment, documents on granting and use of annual leave shall be retained for one (1) year.	FED/MI/TX: No less than three (3) years from date record is created. CA/NY: No less than three (3) years after termination of employment. WA: No regulations so follow FED.	Same as above.	
Appraisals and performance reviews	From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination of the employment but only	Thirty (30) years from the inception date of the documents.	Fifty (50) years.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained ten (10) years from termination of employment.	Six (6) months from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by	FED/MI: No less than three (3) years from date record is created. CA/NY: No less than three (3) years after termination of employment. TX: One (1) year following employee's last day of	Same as above.	

Document	Poland	Romania	Russia	Singapore	Sweden	Switzerland	UK	Ukraine	USA[4] [USA 5]	Vietnam	Korea
	when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)			retention is no longer necessary for legal or business purposes. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).				legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	work. WA: No regulations so follow FED.		
Records relating to promotion	From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination of the employment but only when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)	Thirty (30) years from the inception date of the documents.	Fifty (50) years.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained ten (10) years from termination of employment.	Six (6) months from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	FED/MI: No less than three (3) years from date record is created. CA/NY: No less than three (3) years after termination of employment. TX: One (1) year following employee's last day of work. WA: No regulations so follow FED.	Same as above.	
Reference provided by a former employer	From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination of the employment but only when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)	No statutory retention period.	Russian legislation doesn't contain definition of "references provided by a former employer".	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that Luxoft retain the personal data for no longer than six (6) months unless necessary for legal or business purposes.	Please see comment on Application Forms/CVs above.	No statutory retention period so same as UK.	Six (6) months from receipt.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	FED/CA/MI/TX/WA: No per se statutory retention period so comply with UK standard. NY: Three (3) years from date hiring process is completed or, if hired, no less than three (3) years after termination of employment. If complaint is filed by applicant, then records must be kept until final disposition.	Same as above.	
Summary of record of service (including but not limited: name, position held and dates of employment)	From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination of the employment but only when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)	Thirty (30) years from the inception date of the documents.	During the employment term. Is immediately returned at the last day of employment.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).	Please see comment on Application Forms/CVs above.	Data necessary to establish a work certificate to be retained ten (10) years from termination of employment.	One (1) year from termination of employment (unless the employee has agreed details should be kept longer).	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	FED/MI: No less than three (3) years from date record is created. CA/NY: No less than three (3) years after termination of employment. TX: One (1) year following employee's last day of work. WA: Four (4) years following calendar year in which employment occurred.	Same as above.	
Payroll and tax records	Payroll records and other records concerns employee's remuneration and social rights; from the 1st January 2019 should be kept during	Payroll – fifty (50) years from the end of financial year in which they were made.	Payroll – five (5) years. n case of absence of personal accounts – fifty (50) years. Payroll sheets for insurance	Under the Companies Act, Goods and Service Tax Act, and Income Tax Act: At least seven (7) years, for records relating to accounting periods ending before 1 January 2007; and At least five (5) years, for records relating to accounting periods ending on	For a minimum of seven (7) years. The seven year retention period starts in the year following the expiry of the calendar year in which the accounting year (to which the information relates) was closed.	Ten (10) years from the end of the civil year.	Six (6) years from termination of employment.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no	FED: Three (3) years minimum from date record is created. Recommended six years given statute of limitations. CA: No less than three (3) years after termination of	Five (5) years from the date of filing for accounting records not directly used for making entries	Three (3) years post termination of employment. For tax records, 10 years from the date of filing,

Document	Poland	Romania	Russia	Singapore	Sweden	Switzerland	UK	Ukraine	USA[4] [USA 5]	Vietnam	Korea
	ten (10) years from the date of termination of the employment. Tax records – five (5) years from the end of the tax year in which the tax obligation arose. Five (5) years for any social benefits documents from the transfer of the documents to the Social Security Office.	Tax records – thirty (30) years from the inception date of the documents.	premium transferred to Social Insurance Fund – five (5) years. Payroll correspondence – five (5) years.	or after 1 January 2007. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).				longer than prescribed by legislation on archives. Payroll – ten (10) years or seventy five (75) years in the absence of an order on appointment and change of a salary. Tax records – ten (10) years from the end of the tax year in which the tax obligation arose. Documents on payment of taxes and fees - five (5) years. .	employment. Recommended four years given statute of limitations. MI: None, so follow FED. NY: Not less than six (6) years from date record is created. TX: Four (4) years after the date of the last payroll check (see Texas unemployment compensation statute) WA: Four (4) years following calendar year in which employment occurred.	in accounting books and financial statements; or Ten (10) years from the date of filing for accounting records directly used for making entries in accounting books and financial statements, accounting books and annual financial statements.	in case of investigations and in accordance with practice standards adopted by professional accounting practices.
Records relating to accident or injury at work	The employer is obliged to keep a record determining the circumstances and causes of an accident at work with other post-accident documentation for ten (10) years from making such file.	Records of individually monitored employee exposure to radiation – forty (40) years from the exposure date; shall be kept by occupational medicine entity agreed by the employer.	Fifty (50) years for documents relating to scene of accident; if associated with major material damage and victims – forever (if occurred in scene of accident). If occurred in other entities - five (5) years.	Five (5) years under the Workplace Safety and Health Act. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).	Please see comment on Application Forms/CVs above.	Five (5) years from date of incident.	Three and a half (3.5) years from date of incident.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. E.g. documents (protocols, reports, conclusions) of harmful labour conditions, injuries, occupational diseases - seventy five (75) years; documents (reports, certificates, lists) of injury at the workplace – ten (10) years; acts on investigation of occupational diseases and poisonings – forty five (45) years etc.	FED/NY/WA: Five (5) years following the end of the calendar year that these records cover. [Note: NY Workers' Compensation Board Form C-2F ("Employer's First Report of Work-Related Injury/Illness") must be retained for 18 years. CA/TX: Five (5) years from date of incident. MI: None, so follow FED.	No statutory retention period. However, as the document arguably might contain personal information of the candidate/employee, privacy law suggests that those who collect or process such personal information may store it only for a period as agreed by the candidate/employee.	Three (3) years after date of accident but if the claim for the accident or injury has commenced, to retain until the claim is completed.
"Spent" disciplinary proceedings Warnings	After one (1) year of impeccable work.	After one (1) year of impeccable work.	Three (3) years for characteristics, certificates, memos for brining to disciplinary responsibility. Five (5) years for disciplinary penalty orders.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).	No statutory retention period. In general to the extent records contain personal data such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded.	Data necessary to establish a work certificate to be retained ten (10) years from termination of employment.	Six (6) months for verbal warning and twelve months for written warnings.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. E.g. documents on infringement of internal rules of conduct one (1) year from the date of issue.	FED/MI: No less than three (3) years from date record is created. CA/NY: No less than three (3) years after termination of employment. TX: One (1) year following employee's last day of work. WA: No regulations so follow FED.	Same as above.	Three (3) years post termination of employment
Grievances	From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination of the employment but only when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)	Thirty (30) years from the registration date with the employer.	Five (5) years.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).	No statutory retention period. In general to the extent records contain personal data such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded.	Data necessary to establish a work certificate to be retained ten (10) years from termination of employment.	Six (6) months after resolution of the grievance.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. Documents on labour disputes - five (5) year.	FED/MI: No less than three (3) years from date record is created. CA/NY: No less than three (3) years after termination of employment. TX: One (1) year following employee's last day of work. WA: No regulations so follow FED.	Same as above.	Same as above
Criminal Convictions	Information about employees' criminal convictions can be	No statutory retention period.	Statutory retention period is not specified.	No statutory retention period. Under the Singapore PDPA, an organization must cease to	In general it is prohibited for others than public authorities to process personal data concerning legal	If related to the employment and necessary to establish a work certificate, it might be	Upon [first annual update after] such	For a period that does not exceed the time necessary for the purposes for which such data are	Criminal convictions are regulated by consumer reporting statutes. If	Same as above.	Same as above

Document	Poland	Romania	Russia	Singapore	Sweden	Switzerland	UK	Ukraine	USA[4] [USA 5]	Vietnam	Korea
	gather only in the form of the no-criminal record certificate. The employer's right to demand such certificate must derive directly from the binding legal provisions. From the 1st January 2019 the duration of keeping employee's personnel file will be shortened to ten (10) years from the date of termination of the employment but only when information was transferred to the employees' personnel file. To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)			retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept no longer than it takes for convictions to become "spent" in accordance with the Registration of Criminal Act.	offences involving criminal offences, judgments in criminal cases, coercive criminal procedural measures or administrative deprivation of liberty, even under circumstances where consent is obtained from the data subject.	retained ten (10) years from termination of employment.	convictions becoming "spent" under the Rehabilitation of Offenders Act 1974 unless, exceptionally information is retained to prevent re-employment.	being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. No statutory retention period, so same as UK.	applicant is not hired based on job-related criminal conviction, then follow applicant retention periods. If employee is terminated based on job-related criminal conviction, then follow post-termination personnel record retention period.		
Ex-Employees records	From the 1st January 2019 ten (10) years from termination of the employment (employees' personal records and other documentation related to the employment relationship stored in hard copies), payroll lists, carts with remuneration, or other evidence that can be basis for pension stored in hard copies); To read more about the rules of how to establish duration of keeping employee's personnel file see appendix no. 16 (Poland)	Retention periods mentioned above shall be also applicable for ex-employees.	Fifty (50) years.	No statutory retention period. Under the Singapore PDPA, an organization must cease to retain personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes. We suggest that records be kept for seven (7) years (i.e. the six year limitation period for contractual claims plus one year).	It depends on the information included in the records. No statutory retention period. In general to the extent records contain personal data such records may not be kept for a longer period than "necessary" with regard to the purpose of the processing. The applicable "necessary" retention period is dependent on the information recorded. Please note that the retention period shall in no case be shorter than applicable statutory minimum retention periods (e.g. personal data processed for accounting purposes shall be stored for seven (7) years according to the requirements in the Swedish Accounting Act). Please note that the Swedish Data Protection Authority has provided recommended retention periods during which personal data may be stored. In general employee personal data should be deleted once the employment relationship has ended. However, data may be stored for as long as (i) there is a potential for a dispute between the company and the former employee, or (ii) the information is necessary with regard to administrative purposes e.g. to administer pension payments or to provide references to other employers. In addition, the company may keep factual information for a longer period (as long as the information is still relevant) such as "termination due to redundancy", "dismissal" or "termination for personal reasons"-notes or likewise together with copies of letters of recommendation or grades provided to the employee e.g. for evaluation of re-employment rights.	Data necessary to establish a work certificate to be retained ten (10) years from termination of employment.	Archived for six (6) years and then securely destroyed.	For a period that does not exceed the time necessary for the purposes for which such data are being processed. In any case, personal data shall be processed in a format allowing the identification of individuals but no longer than prescribed by legislation on archives. According to legislation on archives, seventy five (75) years from termination of employment.	Depends on type of record. Generally, archive personnel records for three (3) years and then securely destroy. Payroll records may have a longer retention period. WA: Requires retention of the following information for four (4) years following calendar year in which employment occurred: name, Social Security number, dates of employment, basis upon which wages are paid, location of services, days worked, number of hours worked each day, total gross pay period earnings, specific sums withheld from earnings and purpose of withholding, cause for discharge or separation.	Same as above.	Same as above.

ANNEX B: DELIVERY AND PROCUREMENT

TRANSPARENCY

You should always ensure that LUXOFT GROUP is transparent about the use of personal data of business contacts.

SECURITY

Never send any personal data or background check results to any client, supplier and third party or to your personal, mailbox without prior consultation with Data Protection officer.

Please collaborate with Legal department to clarify the essence of relations with the counterparty.

Please notify Global Data Protection Officer if according to contract or other documentation Luxoft is expected to be responsible for GDPR or other legal compliance of software or services/works provided to client.

If you work with personal data of your colleagues or subordinates: salaries, bonuses, CV, background check data, please pass the training: Personal Data Protection for processors (Lux-053). This training is obligatory for all internal processors of personal data.

Please do always notify and involve the Global Data Protection Officer and Information Security Officer in any projects during which Luxoft will have access to client's personal data (except contact details of client's team) or Luxoft will process client's personal data in its internal systems or Luxoft will transfer its personal data to the client (in addition to Luxoft team's contacts and CVs).

Notify the Global Data Protection Officer in case you communicate with the client indirectly – through some agent or service provider.

It is important for the client to comply with the relevant data protection laws and to satisfy themselves that LUXOFT GROUP entity's procedures are adequate. Please contact the Data Protection Officer if you have any questions regarding personal data in your project. **[Australia 12] [Canada 6] [India 2China 14] [Malaysia 14 and Malaysia 3] [Netherlands 5]**

In case of any doubts regarding personal data, please contact a local lawyer or Global Data Protection Officer: GlobalDataProtectionOffice@luxoft.com.

NEW DATA PROCESSING ACTIVITIES

Before the beginning of any new project involving personal data, project manager must always involve the Global Data Protection Officer to conduct a Privacy Impact Assessment and Legitimate Interest Assessment.

LUXOFT GROUP shall carry out data protection impact assessments ("DPIA") **before introducing some** new personal data processing activities.

TRANSFERS

Any transfer of personal data outside your own jurisdiction or to change the purpose of such transfers, transfer of employees' personal data or client's personal data to other location to be done with the approval of the appropriate Data Protection Officer. **[India 2, India 6 and India 7][China 3] [Malaysia 2] [China 5]**

Notify Global Data Protection Officer about potential or current exchange of personal data between Luxoft in EU and its client or client's representative outside EU. This data transfer requires additional security measures and safeguards.

ANNEX C: INFORMATION TECHNOLOGY DEPARTMENT

LAWFUL PURPOSES

New Uses — Use of data for a new purpose, can also affect LUXOFT GROUP's filings with data protection authorities (e.g. new IT applications or system developments). IT Staff should check that the relevant Department making the request has consulted the Data Protection Officer, if they wish to use personal data for a new purpose. **[India 2 and India 3]** [**France 6] [Malaysia 3]**

DATA QUALITY

Test Data — Where live data is used for test purposes (if at all necessary), such data should where possible be anonymised prior to any such testing.

Data Review — Datasets should be reviewed regularly to ensure data is classified in line with Rules on Company information treatment by employees, Information Security Manual as well as to identify duplicate records, synchronise data, simplify access and streamline databases.

Data retention — Implement the retention periods in intercompany databases according to Supplementary document 3.1 and for local databases according to Supplementary document 3.2.

SECURITY

The Information Technology Department is responsible for assessing the Information Technology requirements to ensure appropriate security and will consult with the other Departments where appropriate. Much of this detail is set out in the Information Security Manual, Security Incident Management and related policies which should be consulted in addition to this document.

The Information Technology Department is responsible for reclaiming any IT equipment from staff who leave and ensuring that any hard drives are wiped.

The Information Technology Department is responsible for ensuring that all laptops and other portable media are encrypted. **[Netherlands 5]**

TRANSFERS

Where any system development or change in the IT services is planned (e.g. relocating data centres, changing IT applications or service providers, adopting new IT solutions and technologies) which may result in a transfer of data, you must seek the input of the appropriate Data Protection Officer. **[India 2, India 6 and India 7] [China 3] [Malaysia 3]**

RIGHTS

The Information Technology Department should action any requests from other Departments to update or correct information held in the databases managed by the Information Technology Department (to the extent that the Departments do not have the appropriate editing rights). **[Sweden 1] [China 5]**

IAD

Before development of any new system or digital process involving personal data, Internal Automation Department must always involve the Data Protection Officer to conduct a DPIA and Legitimate Interest Assessment (LIA).

Information security department

The Information security department is responsible for audits and checks of suppliers' services and for implementation of client's information security requirements. The Information security department participate in contracting process as an approver.

ANNEX D: FACILITIES

DATA PROTECTION SAFEGUARDS

LAWFUL PURPOSES

Requests to disclose data	If you receive a request to forward personal data to a third party such as the police: you should first check with the Head of Personnel Department if it relates to an employee (current or former) and with the Data Protection Officer. They will determine if the release of this data would breach data protection legislation. **[India 2 and India 6][Malaysia 3]**

TRANSPARENCY

If data is collected about employees and / or visitors who access a LUXOFT GROUP entity's premises (e.g. when using a card system): notice about how LUXOFT GROUP uses this information should be included in an employee privacy notice. Save for the use of CCTV, it is not necessary to give notice to visitors as long as LUXOFT GROUP's use of their data is likely to be for expected purposes. **[Australia 13] [Bulgaria 10] [France 12] [China 16] [Malaysia 13] [Singapore 9]**

Notice of CCTV use	If you are responsible for monitoring the security of LUXOFT GROUP's premises by use of CCTV cameras (especially in reception areas and car parks): you will be responsible for ensuring that the CCTV is drawn to the attention of employees, visitors and others who may be recorded by positioning prominent notices wherever the CCTV is used. Before CCTV is introduced into new areas, you must carry out an impact assessment to ensure that there is a business need for monitoring which justifies its use and to ensure that the monitoring is carried out with the minimum of intrusion, and in accordance with any local law requirements. **[Australia 14] [Cyprus 13] [Germany 4] [Luxembourg 9] [Romania 5] [Sweden 10]**
Sensitive Personal Data	If a specific investigation by Facilities requires the processing of sensitive personal data (e.g. if an employee is suspected of criminal activities and CCTV is used to watch that specific individual for evidential purposes), you should seek prior approval from the Data Protection Officer. **[Bulgaria 11] [IndiaChina 2 and India 7] [Malaysia 3]**

RETENTION

If CCTV images are stored, this will be for a maximum period of 30 days. **[China 17]**

Visitor registers should be stored in the locker with limited access and destroyed 3 years after the visitor has been to the building. **[Australia 15] [China 17] [Cyprus 14] [Malaysia 15] [Singapore 10] [Sweden 11]**

DATA QUALITY

You should ensure that there is a clear and foreseeable need for information collected about individuals. For example, CCTV should not be focussed on other non-LUXOFT GROUP private property or on public spaces such as streets. **[Malaysia 16]**

SECURITY

If access to and movement around some of LUXOFT GROUP's premises is monitored for security purposes: system access should be checked from time to time to ensure that there are no suspicious movements. **[Netherlands 5]**

RIGHTS

All requests from individuals to see their data (e.g. request for CCTV images) should be promptly forwarded to the Personnel Department (for employees) and to the Data Protection Officer in other situations. However, these Departments may require you to provide certain information in response to the requests. It is important that CCTV images are kept in a format that enables them to be

provided in response to a request, provided that they have not already been deleted. **[Malaysia 17] [China 5]**

ANNEX E: LEGAL

CONTRACTING

Please read carefully and follow the Data protection rules of contracting set out in the clause 4.9 of this Policy.

You should always ensure that appropriate Data Processing Agreement (see the supplementary documents below) is concluded or data protection clauses are included in contracts with clients and suppliers, where required by Data protection rules of contracting.

Please keep in mind that **'processor'** means a person, which processes personal data **on behalf** of the controller and on **documented instructions** from the controller. Otherwise person/entity is not a processor.

Please contact the DPO if you have any questions regarding the use of Data Processing Agreement or wording.

TRANSFERS

Any new requests to transfer personal data outside your own jurisdiction or to change the purpose of such transfers should only be done with the approval of the appropriate DPO. **[India 2, India 6 and India 7][China 3] [Malaysia 2] [China 5]**

NEW DATA PROCESSING ACTIVITIES

When approve or advice on any new project, involving personal data, do always involve the Global DPO to conduct a Privacy Impact Assessment and Legitimate Interest Assessment.

LUXOFT GROUP shall carry out data protection impact assessments ("DPIA") **before introducing** some new processing activities.

SUPPLEMENTARY DOCUMENT 4: SAMPLE DATA WORDING FOR MSA and NDA

This sample data wording should be used if Luxoft's assigned personnel may have unmeant access to CLIENT Personal data without any further processing of it and if Luxoft provides LUXOFT personal data of the team members to the Client.
In case of actual transfer of personal data to Luxoft filing system, the Parties shall enter into a separate data processing agreement. Please see sample in Supplementary document 5.

DEFINITIONS
"CUSTOMER Personal Data" means any Personal Data transferred by CUSTOMER or on its behalf to LUXOFT and/or processed in connection with this Agreement or any SOW;

"LUXOFT Personal Data" means any Personal Data controlled by LUXOFT (e.g.: names and contact details of team members, working and billing time, CVs, education, work experience, background, assessment, training and test results, feedback grades and other characteristics) and transferred by LUXOFT or on its behalf to CUSTOMER;

"Personal Data" means, without limitation: personally identifiable information or personal data as defined under the laws of the respective jurisdiction applicable to the performed, Services, including the EU Regulation (EU) 2016/679 ("GDPR");, in any event (i) any information that can be used to distinguish or trace an individual's identity, such as person's name, date and place of birth, biometric records mother's maiden name, address, email address, telephone number, social security number, state identification or driver's license numbers, account information, PIN numbers, access and security codes, login information; and (ii) any other information that is linked or linkable to an individual, such as information about a person's sex, age, income, health or medical information, educational, financial and employment information. Personal Data includes whole or partial copies of such information or materials derived from such information;

1. PROTECTION AND RETENTION OF CUSTOMER PERSONAL DATA

1.1. LUXOFT may Process contact Personal Data of key account personnel of CUSTOMER (name, surname, e-mail address and phone number) for commercial communication and quality control, provided the concerned key account personnel concerned has not objected.

1.2. To the extent possible, CUSTOMER shall anonymize or pseudonymize CUSTOMER Personal Data before providing LUXOFT personnel with the access to it.

1.3. If during the term of this Agreement the transfer of non-anonymized CUSTOMER Personal Data to LUXOFT is necessary to provide Services to CUSTOMER, then LUXOFT may collect, use, transfer, store, access or otherwise process (collectively "Process") CUSTOMER Personal Data on behalf of CUSTOMER as its data processor. For this purpose and to the extent required under applicable law, in particular pursuant to Article 28 paragraph 3 of GDPR, LUXOFT and CUSTOMER shall enter into a separate data processing agreement, that sets out the subject-matter and duration of the processing, the list of security measures, the nature and purpose of the processing, the type of CUSTOMER Personal Data and categories of data subjects and the obligations and rights of the CUSTOMER and LUXOFT.

1.4. The Parties agree that LUXOFT's assigned personnel may have unmeant access to CUSTOMER's Personal Data without any further processing of it in the course of providing ancillary services. LUXOFT agrees to take all reasonable steps to oblige assigned personnel to keep CUSTOMER's Personal Data confidential.

1.5. LUXOFT shall take the appropriate physical, technical and organizational security measures to protect the CUSTOMER Personal Data as instructed. Acting as a processor, LUXOFT will process the CUSTOMER Personal Data in accordance with applicable laws.

1.6. CUSTOMER agrees that acting as a processor LUXOFT may: (i) provide access to CUSTOMER Personal Data to its Affiliates in various jurisdictions (listed at: https://www.luxoft.com/luxoft-overview/#location) for legal, administrative and management purposes; (ii) involve its Affiliates as subprocessors in case of subcontracting in accordance with Section 10.2 of this Agreement without prior notice to CUSTOMER; (iii) transfer CUSTOMER Personal Data, to its subcontractors, across country border (outside the European Union), provided that the legal obligations for such transfer are fulfilled and the physical, technical and organizational security measures are maintained on the same level as required by the applicable laws. (e.g. by entering into EU standard contractual clauses).

1.7. LUXOFT will not engage any other third parties than those as set out in Section 8.6 as subprocessors without authorisation of CUSTOMER which shall be deemed given if CUSTOMER does not raise an objection within one (1) week, or such other notice period as may be reasonably required, after LUXOFT has notified CUSTOMER on the intended engagement of such third party subprocessor.

1.8. CUSTOMER warrants that (i) CUSTOMER has the authority to Process CUSTOMER Personal Data and make it available to LUXOFT in connection with the performance of the Services and (ii) that CUSTOMER Personal Data has been Processed in accordance with applicable laws.

1.9. Following the expiration of this Agreement LUXOFT may retain the CUSTOMER Personal Data for such time period as required under the applicable laws.

1.10. As a controller CUSTOMER shall:

- issue and negotiate with LUXOFT the documented instructions for Processing, including without limitation detailed descriptions of LUXOFT's processing obligations. In detail: how, where, how often and during which term LUXOFT may Process Personal Data, lists of processed Personal Data, lists of data subjects, lists of technical and organisational security measures to be implemented by LUXOFT in regard to its filing system and processing activity;
- only transfer accurate and up-to-date CUSTOMER Personal Data to LUXOFT's filing system and continuously update and maintain accuracy of CUSTOMER Personal Data;
- notify each Data Subject (or other controllers of Personal Data) about the transfer of Personal Data to LUXOFT's filing system for further processing, according to points e) and f) of Article 13 (1) GDPR;
- collect explicit and informed consent from each Data Subject before transfer of Personal Data to LUXOFT and its affiliates and sub-contractors worldwide, according to point a) Article 49 (1) GDPR;
- collect any and all consents from Data Subjects in relation to the transfer and processing of Personal Data for the purposes of rendering Services, and retain for a period as determined by applicable laws and regulations (which may extend beyond the termination or expiration of the Agreement);
- provide each Data Subject with LUXOFT's contact details on behalf of LUXOFT according to point a) of Article 13 (1) GDPR.

1.11. If during the term of this Agreement LUXOFT provides CUSTOMER with LUXOFT Personal Data, CUSTOMER as a processor shall:

- represent and warrant that processing provided LUXOFT Personal Data complies with local, and foreign privacy and data protection laws, regulations and directives, including requirements for the localization of citizens' personal data as applicable;

- process LUXOFT Personal Data only as reasonably required for the performance of this Agreement;
- take appropriate physical, technical and organizational measures to keep LUXOFT Personal Data confidential, secure and protect LUXOFT Personal Data against unauthorized or unlawful processing or access or against accidental loss or destruction;
- not use LUXOFT Personal Data for trading, direct marketing or solicitation;
- immediately notify LUXOFT in case of any security breach that exposes LUXOFT Personal Data. CUSTOMER shall fully cooperate with LUXOFT in complying with any laws regarding notification of such security breach.

1.12. The Data Processing Agreement may contain further provisions on the processing of CUSTOMER Personal Data which shall prevail over the provisions of this Agreement.

SUPPLEMENTARY DOCUMENT 5: SAMPLE DATA PROCESSING AGREEMENT WITH THE CLIENT

This Data Processing Agreement template should be used if the Luxoft entity acts as a data processor on behalf of the client (in case of actual transfer of personal data to Luxoft filing system).

Annex [XX] – Data Processing Agreement

This Data Processing Agreement - hereinafter referred to as "Data Processing Agreement" dated ___ _____, 201_ is entered into by and between Luxoft [XX] with its principal place of business at [Address] , including its affiliates – hereinafter collectively referred to as " Processor " – and [Name] with its principal place of business at [Address] - hereinafter referred to as " Controller " –in consideration of the mutual agreements hereinafter contained, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the parties hereto, intending legally to be bound hereby, agree as follows:

Data protection measures

1. The following provisions shall apply whenever Processor processes personal data of the Controller ("**Controller Data**") on behalf of the Controller.

2. Obligations of the Processor

2.1 The Processor shall exclusively process Controller Data within the scope of the LUXOFT "Master Service Agreement" ("**MSA**") dated [XX] and within the limits of the processing purposes and the scope defined in Appendix 1, for the purpose of providing the agreed services to the Controller ("**Services**") during the term of the MSA, as well as pursuant to the instructions of the Controller. The Processor shall not use Controller Data for any other purpose.

2.2 Controller's Personal Data provided by Controller or collected by Processor and/or its affiliates (if any):
Please check the boxes that apply, below.

Type of Personal Data	☐None ☐Employee data ☐Customer data ☐Vendor data ☐**Special categories of personal data:** ☐Racial and ethnic origin ☐Political opinions ☐Religious or philosophical beliefs ☐Union membership ☐Health ☐Sexual orientation ☐Other types of Personal Data Add details here:	Categories of Data Subjects	☐None ☐Employee information ☐Customer information ☐Vendor information ☐End user information ☐Job Applicant information ☐Third party information ☐Other categories of Data Subjects Add details here: Scope, type and purposes of data processing:

2.3 In the performance of its duties under the MSA, Processor shall comply with all measures agreed by the Parties for the protection of the Controller Data.

2.4 The Processor shall assure the contractual compliance with all agreed measures in the area of the processing of Controller Data.

2.5 Documents and files that are no longer required containing Controller Data may only be destroyed in compliance with data protection regulations subject to the prior consent of the Controller, unless they are deleted within the course of standard deletion procedures agreed upon between the parties.

2.6 Upon termination of the MSA, for any reason whatsoever, the Processor shall immediately hand over to the Controller all documents in its possession and the results of processing or usage which relate to the contractual relationship. Controller Data held on the Processor's storage media (including, but not limited to for example hard drives, USB sticks, CD ROMs) shall then be irretrievably and professionally deleted. Test and scrap material shall be destroyed immediately or handed over to the Controller. Hereby, the Controller always respects the statutory regulations.

2.7 The Processor has appointed a data protection officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.

2.8 The Processor shall — insofar as this is possible and taking into account the nature of the data processing operations — assist the Controller by appropriate technical and organizational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in under applicable data protection law, and shall assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of the data processing operations and the information available to the processor. The Controller shall compensate Processor for any costs and expenses incurred by fulfilling this obligation.

2.9 The Processor shall not directly respond to any enquiries of data subjects and shall refer such data subjects to the Controller. Where a data subject requests the Processor to correct, delete or block data, the Processor shall refer such data subject to the Controller without undue delay.

2.10 Processor may transfer Controller Data to a territory which is not a Member State of either the EU or the EEA only in case the specific conditions of Article 44 et seq. GDPR have been fulfilled, i.e. appropriate safeguards in the respective territory or for the data transfer to the data recipient are provided.

3. Subcontracting

3.1 The Processor may commission subprocessors as specified in Sections 3.2 and 3.1.

3.2 The Controller agrees to the commissioning of the following subprocessors on the condition of a contractual agreement in accordance with Article 28 para. 2-4 GDPR:

Subprocessor	Address/country	Service

3.3 The Processor may add or replace subcontractors under the condition that:

a) the Processor informs the Controller of any intended changes concerning the addition or replacement of subcontractors with appropriate advance notice; and
b) the Controller has not objected to the planned addition or replacement of subcontractors in writing or in text form; and
c) the subcontracting is based on a contractual agreement in accordance with Article 28 para. 2-4 GDPR.

3.4 If the subprocessor provides the agreed service outside the EU/EEA, the Processor shall ensure compliance with EU Data Protection Regulations by appropriate measures.

4. Authority to issue instructions

4.1 The Processor is obliged to strictly follow the instructions given by the Controller under the MSA or this Data Processing Agreement as well as those issued on an individual basis with regard to the collection, processing and/or usage of Controller Data. Section **Error! Reference source not found.** of the Data Processing Agreement shall remain unaffected.

4.2 Instructions may only be issued by the Controller's management board, data protection officers and the manager of the Controller's legal department (hereinafter "**Persons authorized to issue instructions**").

4.3 If the Processor holds the view that any instruction contravenes statutory regulations and/or the Data Processing Agreement, the Processor shall be obliged to notify the Controller hereof immediately, and is entitled to suspend execution of the instruction concerned, until the Controller confirms such instruction in writing. The Processor has the right to reject a – also written confirmed – instruction in case the Processor itself would be liable to prosecution if he would execute the instruction.

5. Data Secrecy and Confidentiality

5.1 The Processor entrusts only such employees with the data processing operations outlined in the MSA and this Data Processing Agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work.

5.2 Save as required by law and other than vis-à-vis its subcontractors, the Processor shall not disclose Controller Data without the written authority of the Controller.

6. The Controller's audit rights.

6.1 The Controller shall have the right to audit Processor's compliance with the statutory regulations on data protection and the obligations entered into between the parties (in particular the technical and organizational measures), without interfering with the regular business operations of the Processor. In this respect, the Controller may:

a) Request information and records about the data processing operations and storage of the Controller Data as well as the data processing routines; Processor shall furnish the relevant information and documentation in due course. Processor may satisfy the request by demonstrating that Processor adheres to an approved code of conduct pursuant to Art. 40 GDPR or an approved certification mechanism pursuant to Art. 42 GDPR.
b) In the event the Controller presents tangible facts demonstrating that Processor has acted in breach of its obligations under this DPA, Processor shall – during its regular business hours and upon reasonable prior notice (of at least 3 business days in advance) – grant the Controller access to the work area where the data processing operations takes place.

7. Data security measures

7.1 The Processor shall implement technical and organizational measures ("**TOMs**") in accordance with Article 32 GDPR. Processor may implement alternative adequate measures providing the same level of security as the TOMs. Any significant changes to the TOMs shall be agreed by the Parties in writing.

8. Security breach notifications and other information duties

8.1 The Processor shall notify the Controller of any malfunctions or indications for an infringement of data protection regulations, or in case of irregularities in the processing of Controller Data, including, but not limited to, data security mishaps and presumed or actually traceable data losses.

8.2 To the extent the Controller has to meet information obligations pursuant to Art. 33 and 34 GDPR, the Processor shall cooperate with the Controller. The Parties agree and acknowledge that Art. 33 and 34 GDPR may impose a notification obligation in the event of the loss or unlawful disclosure of personal data or access to it; the Processor shall notify potentially relevant incidents to the Controller immediately and provide the Controller with all reasonably required support (i) in assessing whether a notification obligation may exist, (ii) mitigating any harm to the data subjects concerned and (iii) supporting the Controller in conducting and filing such notification.

8.3 The Processor shall, provided that it is lawful for it to do so, immediately notify the Controller if it receives any request correspondence, notice or other communication whether orally or in writing from a Data Protection Authority or other authority, relating to Controller Data.

9. International Data Transfers

9.1 The Processor shall not transfer Controller Data to any country outside the European Economic Area without the prior written consent of the Controller, such consent may be subject to and given on such terms as the Controller may in its absolute discretion prescribe. Any consent will be conditional upon the transfer being made a) to a country subject to a positive finding of adequacy by the European Commission (Art. 45 para. 3 GDPR) or b) to an organization (i) that has signed up to standard contractual clauses as approved by the European Commission in Decision 2010/87/EU or any successor decision ("**C2P SCCs**") pursuant to Art. 93 para. 2 GDPR, (ii) that is bound by Binding Corporate Rules pursuant to Art. 47 GDPR, (ii) by an approved code of conduct pursuant to Article 40 or (iii) by an approved certification mechanism pursuant to Article 42 GDPR, or c) on the basis of other safeguards pursuant to Art. 46 para. 2 GDPR. Where the Controller provides consent to a transfer of Controller Data subject to the Processor entering into C2P SCCs, it authorizes the Processor to enter into those C2P SCCs on its behalf.

10. Term of the Data Processing Agreement and Precedence

10.1 Unless specifically stipulated to the contrary by the Parties, the duration of the commissioned data processing specified by this Data Processing Agreement shall be in accordance with the provisions on the term of the MSA.

10.2 The terms and conditions of the MSA shall apply subsidiarily to the terms of this Data Processing Agreement. In the event of conflicting provisions, the provisions of this Data Processing Agreement shall prevail.

[place], [date]

_____

Controller

[place], [date]

_____

Processor

SUPPLEMENTARY DOCUMENT 6: SAMPLE DATA PROCESSOR WORDING WITH THE SUPPLIER

If supplier's assigned personnel may have unmeant access to personal data without any further processing of it, then amend the contract with this special wording for minimal data protection.

FOR PURCHASING OF GOODS:

Protection of personal data

a As a result of the engagement, the Parties may have access to personal data of employees, managers, representatives and partners of each other and may need to process this personal data for legal, administrative and management purposes. If Seller is processing personal data, Seller shall:

b only undertake processing of personal data reasonably required in connection with this Agreement and in accordance with the applicable personal data protection laws;

c not use the provided personal data for direct marketing or solicitation;

d take appropriate physical, technical and organizational measures to keep the provided personal data confidential, secure and protect against unauthorized or unlawful processing or access or against accidental loss or destruction;

e immediately notify Buyer if there is any personal data breach that exposes provided data. Seller shall fully cooperate with Buyer in complying with any laws regarding notification of such personal data breach.

FOR PURCHASING OF WORKS AND SERVICES:

Protection of personal data

1. In case Seller (in this clause Seller means Seller and/or any of its Affiliates/representatives) receives or has access to any information relating to an identified or identifiable person ("Personal Data") from Buyer (in this clause Buyer means Buyer and/or any of its Affiliates), Seller will comply with this subsection.
2. The Seller acknowledges that Buyer is the data controller in respect of Buyer's Personal Data that the Seller processes in the course of providing services for Buyer, and that the Seller is the data processor in respect of Buyer's Personal Data.
3. Seller shall ensure that it complies with the provisions and obligations imposed by the applicable legislation relating to data protection.
4. In addition Seller shall be bound by the following obligations with regard to Personal Data received or given access to by Buyer. Seller agrees that it shall:

a) only (i) carry out processing of Buyer's Personal Data in accordance with Buyer's instructions and (ii) comply with instructions from Buyer to rectify, erase and/or block Buyer's Personal Data;

(b) agree with Buyer and implement appropriate technical and organizational measures to protect Buyer's Personal Data against unauthorised or unlawful processing and accidental destruction or loss;

(c) use all reasonable endeavors to advise Buyer if, in the light of new technology and methods of working, Buyer should consider revising the implemented security methods;

(d) not sub-contract any processing of Buyer's Personal Data without the prior written consent of Buyer;

(e) immediately refer to Buyer any requests, notices or other communication from data subjects, data protection authorities or any other law enforcement authority, for Buyer to resolve;

(f) at no additional cost, provide such information to Buyer as Buyer may reasonably require, and within the timescales reasonably specified by Buyer, to allow Buyer to comply with the rights of data subjects, including subject-access rights, or with notices served by any data protection authority;

(g) not transfer any of Buyer's Personal Data outside of the European Economic Area without the prior written consent of Buyer;

(h) represent and warrant that its collection, access, use, storage, disposal and disclosure of Buyer's Personal Data does and will comply with all applicable federal, state, provincial, local, and foreign privacy and data protection laws, as well as all other applicable regulations and directives;

(i) immediately forward to Buyer any requests by data subjects regarding the correction or deletion of Personal Data;

(j) immediately notify Buyer of any monitoring activities and measures undertaken by the supervisory authority;

(k) immediately notify Buyer if the Seller infringes provisions relating to the protection of Buyer's Personal Data. The Parties agree and acknowledge that Art. 33 and 34 GDPR may impose a notification obligation in the event of the loss or unlawful disclosure of Personal Data or access to it; Seller shall notify potentially relevant incidents to Buyer immediately and provide Buyer with all reasonably required support (i) in assessing whether a notification obligation may exist, (ii) mitigating any harm to the data subjects concerned and (iii) supporting Buyer in conducting and filing such notification;

(l) on the termination of this Agreement and at the choice of Buyer, return all of Buyer's Personal Data to Buyer or destroy all of Buyer's Personal Data and certify to Buyer that it has done so, unless prevented from doing so by applicable laws. In that case, the Seller warrants that it will guarantee the confidentiality of Buyer's Personal Data and will not actively process such Personal Data anymore.

(m) Comply with all Instructions, security measures contained in GDPR, maintain all necessary records according to GDPR;

5. Seller agrees to provide Buyer with written confirmation of GDPR compliance on annual basis to the following e-mail GlobalDataProtectionOffice@luxoft.com.
6. The Seller shall, at no additional cost, keep or cause to be kept full and accurate records relating to all processing of Buyer's Personal Data on behalf of Buyer and shall, upon reasonable notice, grant Buyer and its auditors and agents, a right of access to and to take copies of such records in order to assess whether the Seller has complied with its data protection obligations. The Seller shall, upon reasonable notice, allow Buyer and its auditors and agents access to premises and other materials and to its personnel and shall provide all reasonable assistance in order to assist Buyer and its auditors and agents in exercising its audit rights under this Clause.
7. Seller's data protection obligations shall continue throughout the Agreement and for a period of six (6) years thereafter.

SUPPLEMENTARY DOCUMENT 7: SAMPLE DATA PROCESSING AGREEMENT WITH THE SUPPLIER

Set out below is the Sample of data Processing agreement which should be signed when LUXOFT (and also its affiliates) is appointing a service provider who will process personal data on behalf of LUXOFT (e.g archive companies, hosting or support providers, travel and migration agencies, hotlines, external DPOs, survey and testing tools, etc).] These have been drafted to comply with the provisions relating to processors set out in the GDPR. **[China 14] [Malaysia 14] [South Africa 10] [Singapore 8]**.
Additional provisions may be required where LUXOFT, whose data is being processed, is based in Canada, Germany, Luxembourg, Poland, South Africa, Sweden or Switzerland. In this situation, please speak to the Data Protection Officer before using these clauses. **[India 2]**

Data Processing Agreement

This Data Processing Agreement - hereinafter referred to as "Data Processing Agreement" or "DPA" dated ___ _____, 201_ is entered into by and between Luxoft [XX] with its principal place of business at [Address], including its affiliates - hereinafter collectively referred to as "Controller",– and [Name] with its principal place of business at [Address] - hereinafter referred to as "Processor" –in consideration of the mutual agreements hereinafter contained, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the parties hereto, intending legally to be bound hereby, agree as follows:

Data protection measures

1. The following provisions shall apply whenever the Processor processes personal data of the Controller ("**Controller Data**") on behalf of the Controller.

2. Obligations of the Processor

2.1 The Processor shall exclusively process Controller Data within the scope of [XX] ("**Service Agreement**") dated [XX] and within the limits of the processing purposes and the scope defined below, for the purpose of providing the agreed services to the Controller ("**Services**") during the term of the Service Agreement, as well as pursuant to the instructions of the Controller. The Processor shall not use Controller Data for any other purpose.

2.2 Controller's Personal Data provided by Controller and/or its affiliates or collected by Processor (if any):
Please check the boxes that apply, below.

Type of Personal Data	☐None ☐Employee data ☐Customer data ☐Vendor data ☐**Special categories of personal data:** ☐Racial and ethnic origin ☐Political opinions ☐Religious or philosophical beliefs ☐Union membership ☐Health ☐Sexual orientation ☐Other categories of Personal Data: - Add details here:	Categories of Data Subjects	☐None ☐Employee information ☐Customer information ☐Vendor information ☐End user information ☐Job Applicant information ☐Third party information ☐Other categories of Data Subjects Add details here: Scope, type and purposes of data processing:

2.3 In the performance of its duties under the Service Agreement, Processor shall comply with all measures agreed by the Parties for the protection of the Controller Data.

2.4 The Processor shall assure the contractual compliance with all agreed measures in the area of the processing of Controller Data.

2.5 Documents and files that are no longer required containing Controller Data may only be destroyed in compliance with data protection regulations subject to the prior consent of the Controller, unless they are deleted within the course of standard deletion procedures agreed upon between the parties.

2.6 Upon termination of the Service Agreement, for any reason whatsoever, the Processor shall immediately hand over to the Controller all documents in its possession and the results of processing or usage which relate to the contractual relationship. Controller Data held on the Processor's storage media (including, but not limited to for example hard drives, USB sticks, CD ROMs) shall then be irretrievably and professionally deleted. Test and scrap material shall be destroyed immediately or handed over to the Controller. Hereby, the Controller always respects the statutory regulations.

2.7 The Processor has appointed a data protection officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.

2.8 The Processor shall assist the Controller by appropriate technical and organizational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in under applicable data protection law, and shall assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of the data processing operations and the information available to the processor.

2.9 The Processor shall not directly respond to any enquiries of data subjects and shall refer such data subjects to the Controller. Where a data subject requests the Processor to correct, delete or block data, the Processor shall refer such data subject to the Controller without undue delay.

2.10 Processor may transfer Controller Data to a territory which is not a Member State of either the EU or the EEA only in case the specific conditions of Article 44 GDPR have been fulfilled, i.e. appropriate safeguards in the respective territory or for the data transfer to the data recipient are provided.

3. Subcontracting

3.1 The Processor is not permitted to commission further sub-processors without the explicit approval by the Controller in writing.

3.2 In the event the Processor commissions further sub-processors pursuant to Section 3.1, the respective data sub-processing agreement shall contain provisions back-to-back to those of this Data Processing Agreement.

3.3 If a sub-processor involved upon the Processor's explicit approval by the Controller in writing provides the agreed service outside the EU or the EEA, the Processor shall ensure compliance with EU Data Protection Regulations by appropriate measures.

4. Authority to issue instructions

4.1 The Processor is obliged to strictly follow the instructions given by the Controller under the Service Agreement or this Data Processing Agreement as well as those issued on an individual basis with regard to the collection, processing and/or usage of Controller Data. Section 4.3. of the Data Processing Agreement shall remain unaffected.

4.2 Instructions may only be issued by the Controller's management board, data protection officers and the manager of the Controller's legal department (hereinafter "**Persons authorized to issue instructions**").

4.3 If the Processor holds the view that any instruction contravenes statutory regulations and/or the Data Processing Agreement, the Processor shall be obliged to notify the Controller hereof immediately, and is entitled to suspend execution of the instruction concerned, until the Controller confirms such instruction in writing. The Processor has the right to reject a – also written confirmed – instruction in case the Processor itself would be liable to prosecution if he would execute the instruction.

5. Data Secrecy and Confidentiality

5.1 The Processor entrusts only such employees with the data processing operations outlined in the Service Agreement and this Data Processing Agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work.

5.2 Save as required by law and other than vis-à-vis its subcontractors, the Processor shall not disclose Controller Data without the written authority of the Controller.

6. The Controller's audit rights.

6.1 The Controller shall have the right to audit Processor's compliance with the statutory regulations on data protection and the obligations entered into between the parties (in particular the technical and organizational measures), without interfering with the regular business operations of the Processor. In this respect, the Controller may:

c) Request information and records about the data processing operations and storage of the Controller Data as well as the data processing routines; Processor shall furnish the relevant information and documentation in due course. Processor may satisfy the request by demonstrating that Processor adheres to an approved code of conduct pursuant to Art. 40 GDPR or an approved certification mechanism pursuant to Art. 42 GDPR.

d) Request access and the Processor shall – during its regular business hours and upon reasonable prior notice (of at least 3 business days in advance) – grant the Controller access to the work area where the data processing operations takes place.

7. Data security measures

7.1 The Processor shall implement technical and organizational measures ("**TOMs**") in accordance with Article 32 GDPR. Processor may implement alternative adequate measures providing the same level of security as the TOMs. Any significant changes to the TOMs shall be agreed by the Parties in writing.

7.2 Upon request, Processor shall provide suitable evidence to Controller of compliance with these requirements.

7.3 Processor agrees to provide Controller with written confirmation of GDPR compliance on annual basis to the following e-mail GlobalDataProtectionOffice@luxoft.com.

8. Data Breach notifications and other information duties

8.1 The Processor shall notify the Controller of any malfunctions or indications for an infringement of data protection regulations, or in case of irregularities in the processing of Controller Data, including, but not limited to, data security mishaps and presumed or actually traceable data losses.

8.2 To the extent the Controller has to meet information obligations pursuant to Art. 33 and 34 GDPR, the Processor shall cooperate with the Controller. The Parties agree and acknowledge that Art. 33 and 34 GDPR may impose a notification obligation in the event of the loss or unlawful disclosure of personal data or access to it; the Processor shall notify potentially relevant Data Breach to the Controller immediately and provide the Controller with all reasonably required support (i) in assessing whether a notification obligation may exist, (ii) mitigating any harm to the data subjects concerned and (iii) supporting the Controller in conducting and filing such notification.

8.3 The Processor shall, provided that it is lawful for it to do so, immediately notify the Controller if it receives any request correspondence, notice or other communication whether orally or in writing from a Data Protection Authority or other authority, relating to Controller Data.

9. International Data Transfers

9.1 The Processor shall not transfer Controller Data to any country outside the European Economic Area without the prior written consent of the Controller, such consent may be subject to and given on such terms as the Controller may in its absolute discretion prescribe. Any consent will be conditional upon the transfer being made a) to a country subject to a positive finding of adequacy by the European Comission (Art. 45 para. 3 GDPR) or b) to an organisation (i) that has signed up to standard contractual clauses as approved by the European Commission in Decision 2010/87/EU or any successor decision ("**C2P SCCs**") pursuant to Art. 93 para. 2 GDPR, (ii) that is bound by Binding Corporate Rules pursuant to Art. 47 GDPR, (ii) by an approved code of conduct pursuant to Article 40 or (iii) by an approved certification mechanism pursuant to Article 42 GDPR, or c) on the basis of other safeguards pursuant to Art. 46 para. 2 GDPR. Where the Controller provides consent to a transfer of Controller Data subject to the Processor entering into C2P SCCs, it authorises the Processor to enter into those C2P SCCs on its behalf.

10. Term of the Data Processing Agreement and Precedence

10.1 Unless specifically stipulated to the contrary by the Parties, the duration of the commissioned data processing specified by this Data Processing Agreement shall be in accordance with the provisions on the term of the Service Agreement.

10.2 The terms and conditions of the Service Agreement shall apply subsidiarily to the terms of this Data Processing Agreement. In the event of conflicting provisions, the provisions of this Data Processing Agreement shall prevail.

11. Indemnification and liability

11.1 Notwithstanding any of the other provisions in the Service Agreement, Processor shall indemnify, defend, and hold harmless Controller, its directors, officers, employees, affiliates, agents and assigns (each, an "Indemnified Party") from and against any and all loss, expense, cost (including without limitation reasonable attorneys' fees), liability, damage, injury to persons or property, arising from third party claims (collectively, "Claims"), of whatsoever kind or nature, imposed on, incurred by or asserted against any Indemnified Party, resulting from, arising out of, or incurred with respect to (whether directly or indirectly): (i) any Data Breach involving Controller Data in the possession, custody or control of Processor or its agents or sub-processors, (ii) the use, disclosure, or other handling of Controller Data by Processor or its agents or sub-processors, (iii) a breach by Processor of any of its obligations under this DPA or the Data Protection Laws (as defined in Sec.12 below) committed by Processor or its agents or sub-processors.

11.2 Without limiting the foregoing, Processor agrees and acknowledges that any data subject that suffers damage as a result of any of Processor's breach of the obligations hereunder shall be entitled to receive compensation from the Processor for the damages.

11.3 For the avoidance, the Parties agreed that this Sec.11 shall not be subject to any limitation of liability provisions set out in the Services Agreement.

12. Glossary of Terms

Personal data means, without limitation: personally identifiable information or personal data as defined under the laws of the respective jurisdiction, including the EU Regulation (EU) 2016/679; and in any event (i) any information that can be used to distinguish or trace an individual's identity, such as person's name, date and place of birth, biometric records, mother's maiden name, address, email address, telephone number, social security number, state identification or driver's license numbers, account information, PIN numbers, access and security codes, login information; and (ii) any other information that is linked or linkable to an individual, such as information about a person's sex, age, income, health or medical information, educational, financial and employment information. Personal Information includes whole or partial copies of such information or materials derived from such information.

Data Protection Laws:

(a) the EU Regulation (EU) 2016/679 ("**GDPR**"); and

(b) other applicable privacy and data protection laws, regulations and directives, relating to or impacting on the processing of Personal data of a data subject and/or its privacy.

Data Breach means any (including but not limited to intentional, negligent or accidental) breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal data.

[place], [date]

_____

Controller

[place], [date]

_____

Processor

SUPPLEMENTARY DOCUMENT 8: SAMPLE DATA SUB-PROCESSING AGREEMENT

*The following provisions shall apply whenever Luxoft as a Sub-Processor processes personal data of the client [XX] ("**Client**") of the Processor ("**Client Data**") on behalf of the Processor.*

Annex [XX] – Data Sub-Processing Agreement

This Data Sub-Processing Agreement - hereinafter referred to as " Sub-Data Processing Agreement" dated ___ _____, 201_ is entered into by and between Luxoft [XX] with its principal place of business at [Address] - hereinafter referred to as "Processor" – and [Name] with its principal place of business at [Address] - hereinafter referred to as "Sub-Processor" –in consideration of the mutual agreements hereinafter contained, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the parties hereto, intending legally to be bound hereby, agree as follows:

1. Obligations of the Sub-Processor

1.1 The Sub-Processor shall exclusively process Client Data within the scope of the "[XX]" ("**Service Agreement**") dated [XX] and within the limits of the processing purposes and the scope defined in Appendix 1, for the purpose of providing the agreed services to the Processor ("**Services**") during the term of the Service Agreement, as well as pursuant to the instructions of the Processor. The Sub-Processor shall not use Client Data for any other purpose.

1.2 Controller's Personal Data provided by Processor or collected by Sub-Processor (if any):
Please check the boxes that apply, below.

Type of Personal Data	☐None ☐Employee data ☐Customer data ☐Vendor data ☐**Special categories of personal data:** ☐Racial and ethnic origin ☐Political opinions ☐Religious or philosophical beliefs ☐Union membership ☐Health ☐Sexual orientation ☐Other categories of Personal Data: - - - Add details here:	Categories of Data Subjects	☐None ☐Employee information ☐Customer information ☐Vendor information ☐End user information ☐Job Applicant information ☐Third party information ☐Other categories of Data Subjects Add details here: Scope, type and purposes of data processing:

1.3 In the performance of its duties under the Service Agreement, Sub-Processor shall comply with all measures agreed by the Parties for the protection of the Client Data.

1.4 The Sub-Processor shall assure the contractual compliance with all agreed measures in the area of the processing of Client Data.

1.5 Documents and files that are no longer required containing Client Data may only be destroyed in compliance with data protection regulations subject to the prior consent of the Processor, unless they are deleted within the course of standard deletion procedures agreed upon between the parties.

1.6 Upon termination of the Service Agreement, for any reason whatsoever, the Sub-Processor shall immediately hand over to the Processor all documents in its possession and the results of processing or usage which relate to the contractual relationship. Client Data held on the Sub-Processor's storage media (including, but not limited to for example hard drives, USB sticks, CD ROMs) shall then be irretrievably and professionally deleted. Test and scrap material shall be destroyed immediately or handed over to the Processor. Hereby, the Processor always respects the statutory regulations.

1.7 The Sub-Processor has appointed a data protection officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.

1.8 The Sub-Processor shall assist the Processor by appropriate technical and organizational measures for the fulfilment of the Processor's obligation to respond to requests for exercising the data subject's rights laid down in under applicable data protection law, and shall assist the Processor in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of the data processing operations and the information available to the Sub-Processor. The Processor shall compensate the Sub-Processor for any costs and expenses incurred by fulfilling this obligation.

1.9 The Sub-Processor shall not directly respond to any enquiries of data subjects and shall refer such data subjects to the Processor. Where a data subject requests the Sub-Processor to correct, delete or block data, the Sub-Processor shall refer such data subject to the Processor without undue delay.

1.10 Sub-Processor may transfer Client Data to a territory which is not a Member State of either the EU or the EEA only in case the specific conditions of Article 44 et seq. GDPR have been fulfilled, i.e. appropriate safeguards in the respective territory or for the data transfer to the data recipient are provided.

2. Subcontracting

2.1 The Sub-Processor is not permitted to commission further sub-processors without the explicit approval by the Processor in writing.

2.2 In the event the Sub-Processor commissions further sub-processors pursuant to Section **Error! Reference source not found.**, the respective data sub-processing agreement shall contain provisions back-to-back to those of this Data Sub-Processing Agreement.

3. Authority to issue instructions

3.1 The Processor is obliged to strictly follow the instructions given by the Processor under the Service Agreement or this Data Sub-Processing Agreement as well as those issued on an individual basis with regard to the collection, processing and/or usage of Client Data. Section **Error! Reference source not found.** of the Data Sub-Processing Agreement shall remain unaffected.

3.2 Instructions may only be issued by the Processor's management board, data protection officers and the manager of the Processor's legal department (hereinafter "**Persons authorized to issue instructions**").

3.3 If the Sub-Processor holds the view that any instruction contravenes statutory regulations and/or the Data Sub-Processing Agreement, the Sub-Processor shall be obliged to notify the Processor hereof immediately, and is entitled to suspend execution of the instruction concerned, until the Processor confirms such instruction in writing. The Sub-Processor has the right to reject a – also written confirmed – instruction in case the Sub-Processor itself would be liable to prosecution if he would execute the instruction.

4. Data Secrecy and Confidentiality

4.1 The Sub-Processor entrusts only such employees with the data processing operations outlined in the Service Agreement and this Data Sub-Processing Agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work.

4.2 Save as required by law and other than vis-à-vis its subcontractors, the Sub-Processor shall not disclose Client Data without the written authority of the Processor.

5. The Processor's audit rights.

5.1 The Processor shall have the right to audit Sub-Processor's compliance with the statutory regulations on data protection and the obligations entered into between the parties (in particular the technical and organizational measures), without interfering with the regular business operations of the Sub-Processor. In this respect, the Processor may:

e) Request information and records about the data processing operations and storage of the Client Data as well as the data processing routines; Sub-Processor shall furnish the relevant information and documentation in due course. Sub-Processor may satisfy the request by demonstrating that Sub-Processor adheres to an approved code of conduct pursuant to Art. 40 GDPR or an approved certification mechanism pursuant to Art. 42 GDPR.

f) Request access and the Sub-Processor shall – during its regular business hours and upon reasonable prior notice – grant the Processor access to the work area where the data processing operations takes place.

5.2 The Client shall have the same audit rights as stipulated in Section **Error! Reference source not found.**.

6. Data security measures

6.1 The Sub-Processor shall implement technical and organizational measures ("**TOMs**") in accordance with Article 32 GDPR. Sub-Processor may implement alternative adequate measures providing the same level of security as the TOMs. Any significant changes to the TOMs shall be agreed by the Parties in writing.

6.2 Upon request, Sub-Processor shall provide suitable evidence to Processor of compliance with these requirements.

6.3 Sub-Processor agrees to provide Processor with written confirmation of GDPR compliance on annual basis to the following e-mail GlobalDataProtectionOffice@luxoft.com.

6.4 The Sub-Processor may implement alternative adequate measures providing the same level of security as the agreed TOMs. Any significant changes to the TOMs shall be agreed by the Parties in writing.

7. Data Breach notifications and other information duties

7.1 The Sub-Processor shall notify the Processor of any malfunctions or indications for an infringement of data protection regulations, or in case of irregularities in the processing of Client Data, including, but not limited to, data security mishaps and presumed or actually traceable data losses.

7.2 To the extent the Processor has to meet information obligations pursuant to Art. 33 and 34 GDPR, the Sub-Processor shall cooperate with the Processor. The Parties agree and acknowledge that Art. 33 and 34 GDPR may impose a notification obligation in the event of the loss or unlawful disclosure of personal data or access to it; the Sub-Processor shall notify potentially relevant Data Breach to the Processor immediately and provide the Processor with all reasonably required support (i) in assessing whether a notification obligation may exist, (ii) mitigating any harm to the data subjects concerned and (iii) supporting the Processor in conducting and filing such notification.

7.3 The Sub-Processor shall, provided that it is lawful for it to do so, immediately notify the Processor if it receives any request correspondence, notice or other communication whether orally or in writing from a Data Protection Authority or other authority, relating to Client Data.

8. International Data Transfers

8.1 The Sub-Processor shall not transfer Client Data to any country outside the European Economic Area without the prior written consent of the Processor, such consent may be subject to and given on such terms as the Processor may in its absolute discretion prescribe. Any consent will be conditional upon the transfer being made a) to a country subject to a positive finding of adequacy by the European Commission (Art. 45 para. 3 GDPR) or b) to an organization (i) that has signed up to standard contractual clauses as approved by the European Commission in Decision 2010/87/EU or any successor decision ("**C2P SCCs**") pursuant to Art. 93 para. 2 GDPR, (ii) that is bound by Binding Corporate Rules pursuant to Art. 47 GDPR, (ii) by an approved code of conduct pursuant to Article 40 or (iii) by an approved certification mechanism pursuant to Article 42 GDPR, or c) on the basis of other safeguards pursuant to Art. 46 para. 2 GDPR. Where the Processor provides consent to a transfer of Client Data subject to the Sub-Processor entering into C2P SCCs, it authorizes the Sub-Processor to enter into those C2P SCCs on its behalf.

9. Term of the Data Sub-Processing Agreement and Precedence

9.1 Unless specifically stipulated to the contrary by the Parties, the duration of the commissioned data processing specified by this Data Sub-Processing Agreement shall be in accordance with the provisions on the term of the Service Agreement.

9.2 The terms and conditions of the Service Agreement shall apply subsidiarily to the terms of this Data Sub-Processing Agreement. In the event of conflicting provisions, the provisions of this Data Sub-Processing Agreement shall prevail.

10. Indemnification and liability

10.1 Notwithstanding any of the other provisions in the Service Agreement, Sub-Processor shall indemnify, defend, and hold harmless Processor, its directors, officers, employees, affiliates, agents and assigns (each, an "Indemnified Party") from and against any and all loss, expense, cost (including without limitation reasonable attorneys' fees), liability, damage, injury to persons or property, arising from third party claims (collectively, "Claims"), of whatsoever kind or nature, imposed on, incurred by or asserted against any Indemnified Party, resulting from, arising out of, or incurred with respect to (whether directly or indirectly): (i) any Data Breach involving Client Data in the possession, custody or control of Sub-Processor or its agents or sub-processors, (ii) the use, disclosure, or other handling of Client Data by Sub-Processor or its agents or sub-processors, (iii) a breach by Sub-Processor of any of its obligations under this DPA or the Data Protection Laws (as defined in Sec.12 below) committed by Sub-Processor or its agents or sub-processors.

10.2 Without limiting the foregoing, Sub-Processor agrees and acknowledges that any data subject that suffers damage as a result of any of Sub-Processor's breach of the obligations hereunder shall be entitled to receive compensation from the Sub-Processor for the damages.

10.3 For the avoidance, the Parties agreed that this Sec.11 shall not be subject to any limitation of liability provisions set out in the Services Agreement.

11. Glossary of Terms

Personal data means, without limitation: personally identifiable information or personal data as defined under the laws of the respective jurisdiction, including the EU Regulation (EU) 2016/679; and in any event (i) any information that can be used to distinguish or trace an individual's identity, such as person's name, date and place of birth, biometric records, mother's maiden name, address, email address, telephone number, social security number, state identification or driver's license numbers, account information, PIN numbers, access and security codes, login information; and (ii) any other information that is linked or linkable to an individual, such as information about a person's sex, age, income, health or medical information, educational, financial and employment information. Personal Information includes whole or partial copies of such information or materials derived from such information.

Data Protection Laws:

(a) the EU Regulation (EU) 2016/679 ("**GDPR**"); and

(b) other applicable privacy and data protection laws, regulations and directives, relating to or impacting on the processing of Personal data of a data subject and/or its privacy.

Data Breach means any (including but not limited to intentional, negligent or accidental) breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal data

[place], [date]

_____

Processor

[place], [date]

_____

Sub-Processor

[USA 6] SUPPLEMENTARY DOCUMENT 9:

PRIVACY NOTICE
FOR CALIFORNIA RESIDENTS

Effective Date: January 1, 2020
Last Reviewed: December 19, 2019

This **PRIVACY NOTICE FOR CALIFORNIA RESIDENTS** supplements the information contained in the Privacy Notice and Declaration of Consent of LUXOFT and its affiliates (collectively, "we," "us," or "our") and applies solely to the residents of the State of California ("consumers" or "you" or "your"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 ("CCPA"), as amended, and other California privacy laws. Any terms defined in the CCPA have the same meaning when used in this notice.

Please note that certain exemptions apply to your rights and our obligations pursuant to the CCPA. These rights and requirements may not apply in certain situations depending on your relationship with us, our other legal obligations and as otherwise provided for in the CCPA.

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will post the updated notice on our website and update the notice's effective date.

Information We Collect
We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("**personal information**"). In particular, we may have collected the following categories of personal information from consumers within the last twelve (12) months:

- **Identifiers** - A real name, alias, postal address, unique personal identifier, online identifier, internet protocol (IP) address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- **Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))** - A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.
- **Protected classifications characteristics under California or federal law** - Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).
- **Internet or other electronic network activity information** - Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.
- **Geolocation data** - Physical location or movements.
- **Professional or employment-related information** - Current or past job history or performance evaluations

Where We Collect Your Personal Information From
We will collect the personal information described above from one or more of the below sources:

- Directly from you throughout our relationship, including when you complete forms and applications, sign up and/or use our services and websites, or when you visit our offices or attend our events.
- Indirectly from you, for example, from observing your actions on our website.
- From our parent entities, affiliates, subsidiaries and partners
- From third parties that are authorized to share your information with us, for example, from documents that our clients provide to us related to the services for which they engage us.

Use of Personal Information
We may use or disclose the personal information we collect for one or more of the following business purposes:

- To fulfill or meet the purpose described to you when collecting your personal information.
- To provide you with information or services that you request from us.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us.
- To improve our website
- To manage our relationship with you or your business.
- To develop and carry out marketing activities in order to keep our clients informed about our products and services.
- To develop and manage our brand.

- To help maintain the safety, security, and integrity of our websites, software, systems, networks, products, services, databases, other technology assets, and business.
- As necessary or appropriate to protect the rights, property or safety of us, our employees or others.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Disclosures of Personal Information for a Business Purpose
In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

- Identifiers.
- California Customer Records personal information categories.
- Protected classification characteristics under California or federal law.
- Internet or other electronic network activity information
- Geolocation data
- Professional or employment-related information.

We disclose your personal information for a business purpose to the following categories of third parties:

- Our parent entities, affiliates and subsidiaries.
- Service providers who help manage, develop and analyze our business and/or deliver services to us and our clients. These service providers have agreed to confidentiality restrictions and use any personal information we share with them or which they collect on our behalf solely for the purpose of providing the contracted service to us.
- Third parties to whom you or your agents authorize us to disclose your personal information.
- Internet cookie information recipients including Google, Facebook, LinkedIn, YouTube and Twitter (click on each respective link to see that party's privacy policy).

No Sale of Personal Information
California residents may opt out of the "sale" of their personal information. We do not "sell" your personal information as we understand that term to be defined by the CCPA and its implementing regulations.

Access to Specific Information and Data Portability Rights
You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- The business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you.

Deletion Request Rights
You have the right to request that we delete any of your personal information that we collected from you and retained. However, we may retain personal information as authorized under applicable law, such as personal information required as necessary to provide our services, protect our business and systems from fraudulent activity, to debug and identify errors that impair existing functionality, as necessary for us, or others to exercise their free speech or other rights, comply with law enforcement requests pursuant to lawful processes, for our own internal purposes reasonably related to your relationship with us, or to comply with legal obligations. We need certain types of information so that we can provide our services. If you ask us to delete it, you may no longer be able to access or use our services.

Exercising Access, Data Portability, and Deletion Rights
To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request through one of the following methods:

- Toll-free line: +1-888-589-6386
- Email: dpo-us@luxoft.com

You may only request a copy of your data twice within a 12-month period. The request must:

- Provide sufficient information that allows us to verify, to a reasonably high degree of certainty, that you are the person about whom we collected personal information. This may include requesting that you provide us with at

least two or more pieces of personal information to match against personal information about you that we may or may not maintain and which we have determined to be reliable for the purpose of verification.

- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Authorized Agent

Only you, or a person you have designated in writing as your authorized agent, or whom is registered with the California Secretary of State to ace on your behalf, or whom you have provided power of attorney pursuant to California Probate Code sections 4000 to 4465, ("Authorized Agent"), may make a consumer request related to your personal information. You may also make a request on behalf of your minor child.

If you wish to have an Authorized Agent make a request on your behalf, they will need to provide us with sufficient written proof that you have designated them as your Authorized Agent and we will still require you to provide sufficient information to allow us to reasonably verify that you are the person about whom we collected personal information.

Non-Discrimination

You have the right not to be discriminated against for exercising any of your CCPA rights. We will not discriminate against you for exercising your CCPA rights.

Contact Information

If you have any questions or comments about this notice, our Privacy Policy, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

Telephone:	+1-888-589-6386
Website:	www.luxoft.com
Email Address:	dpo-us@luxoft.com
Mailing Address:	Luxoft USA, Inc. 1 Rockefeller Center, Floor 27 New York, NY 10020 USA

[USA 6] SUPPLEMENTARY DOCUMENT10:

PRIVACY NOTICE
FOR CALIFORNIA RESIDENTS (EMPLOYEES)

Effective Date: January 1, 2020
Last Reviewed: December 19, 2019

This **PRIVACY NOTICE FOR CALIFORNIA RESIDENTS (EMPLOYEES)** supplements the information contained in the Privacy Notice for Employees of LUXOFT and its affiliates (collectively, "we," "us," or "our") and applies solely to the residents of the State of California ("consumers" or "you" or "your"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 ("CCPA"), as amended, and other California privacy laws. Any terms defined in the CCPA have the same meaning when used in this notice.

Please note that certain exemptions apply to your rights and our obligations pursuant to the CCPA. These rights and requirements may not apply in certain situations depending on your relationship with us, our other legal obligations and as otherwise provided for in the CCPA.

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will post the updated notice on our website and update the notice's effective date.

Information We Collect
We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("**personal information**"). In particular, we may have collected the following categories of personal information from consumers within the last twelve (12) months:

- **Identifiers** - A real name, alias, postal address, unique personal identifier, online identifier, internet protocol (IP) address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- **Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))** - A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.
- **Protected classifications characteristics under California or federal law** - Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).
- **Internet or other electronic network activity information** - Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.
- **Geolocation data** - Physical location or movements.
- **Professional or employment-related information** - Current or past job history or performance evaluations

Where We Collect Your Personal Information From
We will collect the personal information described above from one or more of the below sources:

- Directly from you throughout our relationship
- Indirectly from you, for example, from observing your actions on our website.
- From our parent entities, affiliates, subsidiaries and partners
- From third parties that are authorized to share your information with us.

Use of Personal Information
We may use or disclose the personal information we collect for one or more of the following business purposes:

- To manage our relationship with you, for example, we use your personal data to pay you, to evaluate your individual performance, and provide benefits in connection with your employment.
- To provide you with information or services that you request from us.
- To provide you with email alerts, event registrations and other notices concerning our services, corporate events or news, that may be of interest to you.
- To improve our website
- As necessary or appropriate to protect the rights, property or safety of us, our employees or others.
- To develop and carry out marketing activities in order to keep our clients informed about our products and services.
- To develop and manage our brand.

- To help maintain the safety, security, and integrity of our websites, software, systems, networks, products, services, databases, other technology assets, and business.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Disclosures of Personal Information for a Business Purpose
In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

- Identifiers.
- California Customer Records personal information categories.
- Protected classification characteristics under California or federal law.
- Internet or other electronic network activity information.
- Geolocation data.
- Professional or employment-related information.

We disclose your personal information for a business purpose to the following categories of third parties:

- Our parent entities, affiliates and subsidiaries.
- Service providers who help manage, develop and analyze our business and/or deliver services to us and our clients. These service providers have agreed to confidentiality restrictions and use any personal information we share with them or which they collect on our behalf solely for the purpose of providing the contracted service to us.
- Third parties to whom you or your agents authorize us to disclose your personal information.
- Internet cookie information recipients including Google (*https://policies.google.com/privacy?hl=en*), Facebook (*https://www.facebook.com/policy.php*), LinkedIn (*https://www.linkedin.com/legal/privacy-policy*), YouTube (*https://www.youtube.com/about/policies/#community-guidelines*) and Twitter (*https://twitter.com/en/privacy*) (click on each respective link to see that party's privacy policy).

No Sale of Personal Information
California residents may opt out of the "sale" of their personal information. We do not "sell" your personal information as we understand that term to be defined by the CCPA and its implementing regulations.

Access to Specific Information and Data Portability Rights
You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- The business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you.

Deletion Request Rights
You have the right to request that we delete any of your personal information that we collected from you and retained. However, we may retain personal information as authorized under applicable law, such as personal information required as necessary to provide our services, protect our business and systems from fraudulent activity, to debug and identify errors that impair existing functionality, as necessary for us, or others to exercise their free speech or other rights, comply with law enforcement requests pursuant to lawful processes, for our own internal purposes reasonably related to your relationship with us, or to comply with legal obligations. We need certain types of information in connection with employment-related activities. If you ask us to delete it, we will not be able to manage the employment relationship, or to meet our legal obligations.

Exercising Access, Data Portability, and Deletion Rights
To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request through one of the following methods:

- Toll-free line: +1-888-589-6386
- Email: dpo-us@luxoft.com

You may only request a copy of your data twice within a 12-month period. The request must:

- Provide sufficient information that allows us to verify, to a reasonably high degree of certainty, that you are the person about whom we collected personal information. This may include requesting that you provide us with at least two or more pieces of personal information to match against personal information about you that we may or may not maintain and which we have determined to be reliable for the purpose of verification.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Authorized Agent
Only you, or a person you have designated in writing as your authorized agent, or whom is registered with the California Secretary of State to ace on your behalf, or whom you have provided power of attorney pursuant to California Probate Code sections 4000 to 4465, ("Authorized Agent"), may make a consumer request related to your personal information.

If you wish to have an Authorized Agent make a request on your behalf, they will need to provide us with sufficient written proof that you have designated them as your Authorized Agent and we will still require you to provide sufficient information to allow us to reasonably verify that you are the person about whom we collected personal information.

Non-Discrimination
You have the right not to be discriminated against for exercising any of your CCPA rights. We will not discriminate against you for exercising your CCPA rights.

Contact Information
If you have any questions or comments about this notice, our Privacy Policy, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

Telephone:	+1-888-589-6386
Website:	www.luxoft.com
Email Address:	dpo-us@luxoft.com
Mailing Address:	Luxoft USA, Inc. 1 Rockefeller Center, Floor 27 New York, NY 10020 USA

COUNTRY APPENDICES:

1. AUSTRALIA

1. Personal information pursuant to the Privacy Act 1988 (Cth) (the "Privacy Act") means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not. "Individual" means a natural person. Entities must comply with the Australian Privacy Principles ("APPs") which are specified in a schedule to the Privacy Act.

2. In Australia there is no requirement to notify the processing of data to any data protection authority.

3. Sensitive information under the Privacy Act also includes membership of professional or trade association, membership of a political association, criminal record, genetic information about an individual that is not otherwise health information or biometric information that is used for the purpose of automated biometric verification or biometric identification or biometric templates. Sensitive information can only be collected with the individual's consent and if the information is reasonably necessary for one or more of the entity's activities, subject to limited exceptions specified in APP 3.

4. In Australia there is an employee record exemption which means that a record of personal information relating to the employment of an employee which is collected by an employer of that employee is exempt from the provisions of the Privacy Act. Examples of such personal information include terms and conditions of employment, the employee's personal and emergency contact details, the employee's performance or conduct, the employee's salary or wages. On this basis, transparency with respect to an employee record is not a requirement under the Privacy Act, however, the Fair Work Act 2009 (Cth) regulates the handling and access to employee records. In addition, where an entity proposes to disclose personal information or sensitive information of an employee to a third party or an associated entity overseas, the requirements of the Privacy Act would apply. It should be noted that job applicants and prospective employees do not fall within the employee records exemptions and are covered by the Privacy Act.

5. In Australia, when an entity collects personal information from an individual, it must inform the individual if it is likely to disclose the data outside Australia and, if practicable, to specify the countries where it is likely to be disclosed.

6. There are no specific exceptions to requirements for transparency and notification for business contact information. If it is not practicable to provide the prescribed information at the time of collecting information, the entity must provide information that is reasonable in the circumstances as soon as practicable after collecting the information.

7. The principles set out in section 4.6 are consistent with the Privacy Act and APP 8 in relation to cross-border disclosure of personal information outside Australia. Before an entity discloses personal information about an individual to an overseas recipient, including an associated or group entity, the entity must either take reasonable steps to ensure that the overseas recipient does not breach the Privacy Act or expressly inform the individual that if he or she consents to the disclosure of information the entity will not need to take reasonable steps to ensure that the overseas recipient does not breach the Act and after being so informed the individual consents to the disclosure. Staff should seek the input of the Data Protection Officer if you are not sure whether a data transfer agreement is in place to facilitate the transfer of personal data out of Australia to a third party or country.

8. Criminal records are considered sensitive information for the purposes of the Privacy Act. See note 3. In addition, while not prohibited, requesting criminal offence data can result in the risk of allegations of discrimination if it is not relevant to the position.

9. Information that forms part of an employee record is exempt from the provisions of the Privacy Act. However, an employee has the right to access certain employee records under the Fair Work Act 2009 and associated regulations. In the case of job applicants or candidates, where the individuals do not become employees, the information does not fall within the employee record exemption and accordingly is subject to the Privacy Act and individuals have a right to request to access such information.

10. In some states, monitoring of computer systems and emails and by CCTV may require specific notice periods, and in some cases consent, from employees under workplace surveillance legislation.

11. The agreement should specify that consent is required before the Service Provider transfers any Personal Data outside Australia.

12. The Privacy Act does not distinguish between data controllers and data processors and all parties that collect or hold personal information are bound by the requirements of the Privacy Act. Client contracts should include

appropriate warranties and indemnities from clients that the client has obtained all relevant permissions, provided notifications and complied with the relevant privacy laws when collecting personal information provided to the LUXOFT GROUP entity for processing.

13. Personal data collected from visitors is subject to the notification requirements under the APPs. We recommend that visitors are provided with purpose notification language prior to the LUXOFT GROUP collecting, using or disclosing their personal data when they visit the premises.

14. In addition to notification requirements under the Privacy Act, workplace surveillance laws in some states require specific notice periods or consent before surveillance of employees commences.

15. Personal information must be destroyed or de-identified if it is no longer needed for a purpose permitted by the APPs and it is not required to be retained under an Australian law or court or tribunal. Therefore the 3 year period must be justified.

2. BULGARIA

1. Bulgarian law does not specify that personal data relate to *living* individuals. Any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, will be considered personal data regardless whether the data subject is dead or alive.

2. The application of the legitimate interests as lawful grounds for personal data processing is very restricted. Although Bulgarian law lists the legal interests among the grounds for data processing, in practice most of the data controller's legitimate interests will not be considered to prevail the interests of the individuals concerned. Usually, the applicable legal grounds for lawful data processing are (1) the data subject's consent; (2) the necessity of the processing for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; and (3) compliance with legal obligations.

3. Data concerning human genome is also explicitly defined as sensitive data under Bulgarian law.

4. It is also necessary to provide information about the representative of the data controller and the categories of data which will be processed.

5. In Bulgaria, generally, employers shall not collect details about illnesses (only absence information), except in cases where such collection and processing of data concerning data subjects' health is necessary for compliance with obligations under labour legislation. Processing sensitive data is generally prohibit unless it concerns the cases explicitly enumerated in the law or there is explicit consent by the data subject.
6. The use of data for a new purpose may also require data subjects' consent.

7. The confidentiality of the correspondence (including emails) is protected by the Constitution of the Republic of Bulgaria. The employer cannot read emails if it knows that it concerns private matters. Since the European court of human rights, by its binding ruling of September 2017, limited employers' right to monitor work emails without prior explicit notification and there is also no specific Bulgarian regulation on work emails, it is highly recommendable to ensure that employees are aware that they cannot use their work email addresses for private purposes and to explicitly prohibit such a use.

8. Under Bulgarian law, each data controller should carry out an impact assessment and on the basis of this impact assessment should determine the respective level of protection of the processed personal data. Depending on the determined level of protection, the data controller should implement respective minimum technical and organizational measures for protection of the personal data. For this purpose the data controller should adopt special Internal Rules (Instruction) on the technical and organizational measures for protection of the personal data.

9. Using CCTV is allowed only if the data subjects are notified in advanced and (i) they have explicitly consented it, or (ii) the company pursues legitimate interest or (iii) there is statutory ground for CCTV application.

10. It is not permitted to collect criminal conviction data unless it is explicitly provided for by Bulgarian statutory provisions.

3. CANADA

1. In Canada (Province of Quebec), personal data should generally be collected from the individual concerned, except with the individual's consent or as authorized by law. If the source of the information is a legal person (e.g. a company), a mention to this effect should be included in the file. Please speak to the Data Protection Officer before collecting personal data from a third party without the individual's consent.

2. Personal health information and financial information is generally considered to be sensitive data in Canada.

3. In Canada (Province of Quebec), when the LUXOFT GROUP collects personal information from an individual, it must, when establishing a file on that individual, also inform the individual of the location where the file will be kept.

4. In Canada (Province of Alberta), when the LUXOFT GROUP entity uses a service provider (including an affiliate) outside Canada to collect, use, disclose or store personal data for or on behalf of the entity, it must include, in its policies and practices relating to processing of personal data, information regarding the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and the purposes for which the service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization. Written information about these policies and practices must be made available on request.

5. It is usually not permitted to collect criminal conviction data unless the job specifically requires it (e.g. financial crimes for a cashier).

6. Prescribed consent and content requirements apply under Canadian anti-spam legislation when sending commercial electronic messages that have a promotional purpose as one of their purposes to an email address. Please speak to the Data Protection Officer before sending such messages.

4. CHINA

1. “Personal Data" or "Personal Information" under the China Cyber Security Law and other applicable laws and regulations governing the protection of personal information in China is defined as all kinds of information which can be used, either alone or together with other information, to identify a natural person's personal identity, including but not limited to name, date of birth, identification numbers, personal biometric information, address, telephone numbers, account number and passwords.

2. In China, there is no separate definition of "sensitive personal data" under applicable laws and regulations. A Guideline (Information Security Technology – Guidelines for Personal Information Protection within Information System for Public and Commercial Services" issued by the State Administration of Standardisation provide that sensitive data such as personal ID card number, mobile number, data relating to race, political affiliation, religion, genetics and fingerprint are regarded as sensitive data, and specific requirements e.g. express consent should be obtained for the use and processing of sensitive data. However, the Guidelines do not have the force of law and are not legally binding.

3. Transfer of personal information to jurisdictions outside of China is generally regarded as a type of "use" of personal information and would be subject to notification and consent requirements. In particular, the consent of data subjects must be obtained. In addition, it should be noted that the PRC State Secret Law expressly prohibits information that constitutes "state secret" to be transferred outside of the PRC without the approval of the National Administration for the Protection of State Secrets. The term "state secret" is widely defined as matters which have a vital bearing on state security and national interests. Further, the Cyber Security Law imposes restrictions on cross-border transfer and obligations on security assessments which may be relevant to transfer of data by LUXOFT GROUP out of China. The exact requirements, and whether the requirements will be applicable to LUXOFT GROUP, will depend on implementation rules and regulations to the Cyber Security Law which are pending. LUXOFT GROUP should monitor the legal developments in this regard prior to conducting any transfer of personal information outside of China.

4. In China, there is no local data protection authority and no notification obligation on processing of personal data to any regulator. There is no requirement to appoint a Data Protection Officer.

5. In China, processing of personal data is subject to obtaining consent from the data subjects. There is no legitimate interest exception, and processing for compliance with legal obligation is not a ground for not obtaining consent.

6. The applicable data protection laws and regulations are silent on whether express or implied consent is required. In practice, it would be prudent for LUXOFT GROUP to obtain express consent where possible.

7. There are no specific exceptions to requirements for transparency, notification and consent for business contact information.

8. Data retention obligations are subject to applicable provisions of laws and regulations relating to data retention of specific data. There is no general obligation not to retain personal data for longer than necessary for the purposes for which the data was collected.

9. Where there is security breach, LUXOFT GROUP has additional obligations to report the breach to the relevant competent departments under the Cyber Security Law. LUXOFT GROUP should set up internal procedures for ensuring that such reporting obligations are met.

10. There is no legal requirement to enter into agreements similar to the European Commission approved agreements regulating transfer of data within LUXOFT GROUP of companies.

11. There is no legal right available to individuals in China to appeal or object to the use of automated decisions to take decisions about them.

12. Consent of employees is required prior to conducting any employee monitoring.

13. As indicated in (5) above, processing of personal data is subject to obtaining consent of data subjects, and not just notification. The Sample Privacy Notice For Employees should include a proviso that LUXOFT GROUP processes personal data subject to obtaining consent from the employees. An additional consent at the end of the Notice should specifically refer to consent for the use of personal data for the processing contemplated in the Notice.

14. There is no distinction under applicable data protection laws and regulations between a data user/controller and a data processor. Data processors who process personal data are directly subject to the data protection obligations under applicable law and regulations. This does not prevent data controller/user to enter into contractual obligations on data processors as has been done in Supplementary Document 4. However it should be noted that this does not relieve the obligations on the LUXOFT GROUP as data transferor.

15. As indicated in (3) above, processing of personal data in China is subject to the requirement to obtain consent from relevant individuals. An additional obligation should be imposed to Clause 1.3 of the Supplementary Document 4 to include an obligation on the Service Provider to assist LUXOFT Entity obtain all consent necessary regarding the processing or use (including transfer) of LUXOFT Entity's Personal Data.

16. There is no consent exception for visitors under applicable laws and regulations on data protection in China. Visitors should be provided with purpose notification language and their consent obtained prior to the Company collecting, using or disclosing their personal data when they visit the premises.

17. There is no prescribed statutory retention period in respect of CCTV images and visitor records.

5. CYPRUS

1. 4.1.2 should be amended as follows (amendments printed in italic): Generally, staff may process personal data (other than sensitive personal data) (1) where this is necessary for LUXOFT GROUP's legitimate interests (as defined by local law), provided this does not cause unreasonable prejudice to the interests of the individuals concerned *and provided that LUXOFT GROUP's interests are not overridden by the interests for fundamental rights and freedoms of the data subjects requiring protection under the European Data Protection Directive and Cyprus local law implementing the same* and (2) where processing is necessary to comply with a legal obligation.

2. In Cyprus, the commission or alleged commission of any criminal offence, criminal prosecution and criminal convictions are sensitive personal data.

3. If personal data are transferred out of the EEA or Switzerland, the permission of the Cyprus Personal Data Commissioner will have to be obtained.

4. In Cyprus you cannot collect details about illnesses unless you obtain the data subject's consent. You can collect details about the health/ illnesses /medical condition without the data subjects consent if the following conditions are met:
   (i) Data are processed by a health professional who is subject to obligations of professional secrecy; and
   (ii) Processing is absolutely required for medical purposes, in order to prevent illnesses, diagnose illnesses and treat illnesses at working places.
   In addition, sickness records should be kept separately from other records containing personal data.

5. You must inform employees of the purpose of collection / processing of such data.

6. It is not usually permitted to collect criminal conviction data unless the job specifically requires it and you must inform the employees in advance / prior to collection of the data of the purpose of collection. Collection of such data must be made according to the provisions of the Cyprus Police Law, Law No. 73(I)/2004 (which provides that excerpt of criminal record kept by the Cyprus police may be given only to the data subject or to third parties to which the data subject has provided authorisation to obtain the excerpt of his/ her criminal record).

7. You must explain to unsuccessful applicants if you want to keep CVs on file for future use and CVs should only be retained if the applicant gives explicit consent.

8. Notes may be considered as personal data and be subject to the same protective regime as personal data.

9. You need explicit consent from employees to send to them direct marketing material.

10. Employees have a right to be informed in advance of the purposes of disclosing personal data to third parties, the personal data to be disclosed and the identity of the recipient third parties of such data. You may also be required to obtain employees' consent. LUXOFT GROUP may disclose freely personal data to third parties (without the data subject's consent) if LUXOFT GROUP has a legal obligation to disclose this information or information is required for legal proceedings or in connection with the prevention or detection of crime.

11. Employees must be notified in ALL circumstances of the purpose, type and duration of the monitoring before monitoring commences. Secret monitoring is not permissible.

12. The Employer cannot read / have access to the content of personal emails of employees and personal phone calls of employees.
13. Emails which are marked as personal should not be read even in exceptional circumstances. LUXOFT GROUP may prohibit the use of its email systems for personal use by its employees. LUXOFT GROUP may adopt a policy for the use of internet and telephone specifying the meaning of the terms business use and personal use.

14. Before CCTV is introduced you must seek guidance from the Data Protection Officer. Employees must be notified in all circumstances of the purpose and duration of monitoring before monitoring commences. Secret monitoring is not permissible.

15. Retention period of 3 years may be considered as excessive under Cyprus law.

6. DENMARK

a. The Danish Law on Processing of Personal Data ("**PDA**") does not restrict the definition of personal data to *living* individuals. Any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, will be considered as personal data regardless whether the data subject is dead or alive.

b. Personal data, which is processed, must be relevant and sufficient and limited to what is necessary in relation to the purposes for which it is processed.

c. Under the PDA a data subject has the right to request access, to object to the processing and to request the controller to correct, block or erase such personal data that has not been processed in accordance with Danish law.

d. Processing of semi-sensitive and sensitive personal data, cf. note 6, requires an authorization from the Danish Data Protection Agency ("**DPA**"). The PDA does not require a data protection officer.

e. Under the PDA the data controller may process ordinary personal data when for instance the processing is necessary to pursue a legitimate interest of the controller and this interest is not overridden by the interests of the data subject.

f. In Denmark information about criminal offences, significant social problems and other purely private matters (other than those mentioned as sensitive personal data) are considered as semi-sensitive personal data. Significant social problems are for instance information about social benefits. Other purely private matters are for instance family disputes, adoption, suicide, separation and severe violation of terms of employment.

g. When collecting personal data, the following information must also be provided: name and address of the respective LUXOFT entity describing that this entity is the data controller, name and address of any representative of the data controller and any other necessary information in order for the data subject to safeguard his/her interests.

h. In Denmark, when an entity collects personal data, it must inform the data subject if it is likely to disclose the data outside Denmark and specify the countries to which it will be disclosed (if the transfer is based on the data subject's consent only). If the transfer is based on SCCs, the controller must inform that it has taken steps to ensure that there is adequate protection for personal data in these circumstances.

i. The requirement to notify the data subject does not apply if the information is already known to the data subject. If the personal data is not provided by the data subject, the requirement to notify the data subject does not apply if notification is impossible or disproportionately difficult.

j. There is no mandatory obligation to notify the DPA. However, it is in some cases considered as good data processing practice to notify the data subject.

k. The conditions set out in section 4.6 are consistent with the PDA in relation to disclosure of personal data outside the EEA. Before an entity discloses personal information about an individual to an recipient established outside the EEA, including an associated or group entity, the entity must either make sure that the recipient ensures an adequate level of protection of personal data or expressly inform the individual that if he or she consents to the disclosure of information the entity will not need to ensure an adequate level of protection of personal data, and after being so informed the individual consents to the disclosure. The entering into EU Commission Standard Contractual Clauses ("**SCCs**") will provide an adequate level of protection of personal data. Please note that the Danish DPA considers even the smallest changes of the SCCs (e.g. changing commas and full stops) as "changes" which makes the SCCs "ad-hoc-contracts", which need authorization prior to the transfer commences. Further, the Danish DPA does not accept multi-signed SCCs. An individual SCC between each exporter and each importer should be made.

l. Processing of personal data is allowed when the processing is necessary in order to fulfil the employment contract between LUXOFT and the data subject. Processing of personal data in the workplace with consent as legal ground shall be limited to situations where the employee is provided with a de facto choice of whether he/she should accept the processing or not and where the employee at a later stage may withdraw his/her consent without facing any negative consequences.

m. Criminal records are considered semi-sensitive information. See note 6. In addition, while not prohibited, requesting criminal offence data can result in the risk of allegations of discrimination, if it is not relevant to the position.

n. If LUXOFT GROUP wishes to keep the data for future recruitment needs, the candidate must be informed accordingly and give his/her consent. Otherwise the data must be deleted as soon as possible and no later than 6 months after the refusal.

o. Pursuant to the PDA, monitoring of employees requires consent from the employee or a necessary operational reason. Further, the purposes of the monitoring should be assessed, and the employer should notify the employees of the monitoring prior to the monitoring. If the employees are employed under collective agreements, certain requirements regarding notification to the employees and the works council (if such council is in fact formed) may likely apply. For instance, the employer is obligated to inform and consult with the works council about the monitoring. This obligation has an informative purpose only. Further, a 6 weeks' prior notice before launching the monitoring should be observed. An individual employee cannot give binding consent to monitoring, if the employee is employed under a collective agreement. Please note that it is prohibited to read any private e-mails, documents or folders.

7. INDIA

- According to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information Rules,2011) (hereinafter referred to as the "Privacy Rules"), Sensitive Personal Data or Information also includes passwords; financial information such as bank account or credit card or debit card details and/or other payment instrument details; information regarding physical, physiological and mental health conditions; medical records and history; biometric information; any detail relating to the foregoing as provided to the LUXOFT GROUP for providing any service(s); and any of the aforementioned information received by LUXOFT GROUP for processing or storage, whether under a lawful contract or otherwise:
- The Privacy Rules further provide that any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.
- In India, there is no legal requirement to appoint a Data Protection Officer. However, LUXOFT GROUP shall address any discrepancies and grievances of the data subject, with respect to processing of information, in a time bound manner and shall designate a Grievance Officer for this purpose and publish his/her name and contact details on its website. The Grievance Officer shall redress the grievances of the data subject expeditiously and shall ensure that it is done within one (1) month from the date of receipt of grievance;
- The Privacy Rules mandate that Sensitive Personal Data or Information shall not be collected, unless the said information is to be collected for a lawful purpose which is connected with a function or activity of the collector; and the collection of such information is necessary for that purpose. The information so collected may be used only for the purpose for which it has been collected. The Privacy Rules further mandate that the LUXOFT GROUP shall put in place a privacy policy (containing the prescribed particulars) for handling of or dealing in personal information and sensitive personal information, shall ensure that it is available for view by the data subjects and shall publish the same on its website.
- The Privacy Rules mandate that the LUXOFT GROUP shall, prior to the collection of information including Sensitive Personal Data or Information, provide an option to the data subject not to provide the data or information sought. Should the data subject choose to provide Sensitive Personal Information, that the LUXOFT GROUP shall, prior to collection of Sensitive Personal Data or Information, obtain from the data subject, consent in writing by way of letter, fax or e-mail regarding the purpose for its use. The data subject shall, at any time have an option to withdraw his/her consent. Such withdrawal of the consent shall be sent in writing to the concerned department in the LUXOFT GROUP. In the case of the data subject not providing or later withdrawing his/her consent, the **LUXOFT GROUP shall have the option not to provide goods or services for which the said information was sought.** *[Note: The Privacy Rules allow the data subject the option to refuse to provide information or to withdraw consent once given. In light of the same the LUXOFT GROUP should determine the course of action to be adopted in the event the data subject refuses to provide data or later withdraws consent.]*
- The Privacy Rules mandate that while collecting information directly from the data subject, the LUXOFT GROUP shall take such steps as are, in the circumstances, reasonable to ensure that the data subject is aware of— (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information.
- The Privacy Rules mandate that the LUXOFT GROUP shall not publish Sensitive Personal Data or Information that it has collected and further mandates that any disclosure of Sensitive Personal Data or Information collected from a person under a lawful contract, to a third – party, shall require the prior permission of the data subject, unless the disclosure thereof has been agreed to by the data subject, in the said contract or where the disclosure is necessary for compliance of a legal obligation. Sensitive Personal Data or Information can also be disclosed to mandated government agencies without prior consent of the data subject or to a third party by an order under the law for the time being in force. The Privacy Rules specify that any third party receiving such Sensitive Personal Data or Information shall not disclose it further.
- The Privacy Rules also mandate that the LUXOFT GROUP may transfer Sensitive Personal Data or Information only if it is necessary for the performance of the lawful contract between the LUXOFT GROUP and the data subject or where such person has consented to the transfer of such information.
- The Privacy Rules mandate that the LUXOFT GROUP shall comply with reasonable security practices and procedures with respect to Personal Data, including Sensitive Personal Data as follows:
  (i) A comprehensive documented information security programme and information security policy that contains managerial, technical, operational and physical security control measures that are commensurate with the data or sensitive personal data being protected with the business is to be implemented;

  (ii) In the event of an information security breach, the LUXOFT GROUP shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law that security control measures have been duly executed as per the documented information security programme and information security policy;

  (iii) Security practices and standards such as the international standard IS/ISO/IEC 27001 on "Information Technology -Security Techniques -Information Security Management System or other codes of best practices duly approved and notified by the central government of India shall be implemented;

(iv) Such standards or codes of best practices are to be certified or audited on a regular basis by entities or an independent auditor, duly approved by the central government. Such audit shall be carried out at least once a year or as and when the LUXOFT GROUP undertakes a significant upgradation of its processes and computer resources.

8. ITALY

- The Italian Parliament recently passed Law No. 163/2017 (Enabling Law) to prepare for the entry into force of Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)), which will be directly applicable in all EU member states as of 25 May 2018.

- The Data Protection Code grants rights to data subjects (natural persons) and imposes certain obligations on the following persons:

• Data controller. The data controller is the natural or legal person, public body or other entity who, alone or jointly with others, determines the purposes and means of processing of personal data, including security measures.
• Data processor. The data processor is the natural or legal person, public body or other entity who processes data on behalf of the data controller on the basis of instructions provided by the data controller.
• Person in charge of the data processing. This is the natural person in charge of the data processing on behalf of either the data controller or the data processor. The instrument appointing such a person and the instructions provided must be made in writing.

- Data controllers must notify the Italian Data Protection Authority (IDPA) before starting data processing activities if either (*Data Protection Code*):

• The data processing concerns certain types of data (such as genetic and biometric data or other data disclosing the geographic location of individuals or objects).
• Personal data is processed for certain purposes (such as profiling purposes or to assess creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful or fraudulent conduct).
The exemptions:
• Non-systematic processing activities of genetic and/or biometric data carried out by healthcare professionals, concerning data that is not organized in a database accessible to third parties via electronic networks and to the extent that the processing is necessary for the purposes of safeguarding the data subject's and/or third party's health.
• Processing of personal data disclosing the geographic position of air, sea, and ground transportation channels, where it is only carried out for the purposes of transport security.
• Processing of personal data relating to the data subject's creditworthiness, provided that such data is stored in databases used for certain purposes, such as in connection with the provision of goods or services, or to comply with accounting or tax requirements or regulatory obligations.

- Data controllers have the following main obligations (*Data Protection Code*):

• Information notice. Before any data processing, data controllers must provide the data subject with information relating to the data processing, the mandatory content of which has been expanded by the General Data Protection Regulation (GDPR)
• Principles for data processing. When processing personal data, data controllers must comply with the following principles:
• lawfulness and fairness: data must be processed lawfully and fairly;
• purpose limitation: data must be collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is compatible with the original purposes;
• accuracy: data must be accurate and, where necessary, kept up to date;
• proportionality: data must be relevant, complete and not excessive in relation to the purpose for which the data is collected or subsequently processed;
• storage limitation: data must be kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data is collected or subsequently processed.
• Implementation of security measures. Data controllers must implement minimum and appropriate security measures to ensure data security.

- Personal data processing operations carried out by private or profit-seeking public bodies require the prior consent of data subjects, in relation to the processing as a whole or to one or more processing operations (*Data Protection Code*).Consent is validly obtained if it is: Freely given; Specific in relation to a clearly identified data processing; Informed. Consent can also be given online, provided that it meets the above conditions.
- The data controller must provide an information notice to the data subject that indicates (Data Protection Code):

• The purposes and means of the data processing.
• Whether providing the personal data is a mandatory or optional requirement.
• The envisaged consequences of failure to provide such data.

• The recipients or categories of recipient of the personal data.
• The rights granted to data subjects.
• The identity of the data controller (and of its representative in Italy, if applicable).
• The identity of the data processor (if any).

– Data subjects have the following rights (Data Protection Code):

• Right to be informed of the:
• source of the personal data;
• purposes and means of the processing;
• logic applied to data processing carried out through electronic means;
• identity of the data controller, data processor (if appointed) and established representative; and
• third parties or categories of third parties to whom the data may be communicated;
• Right to have their data updated, rectified or integrated.
• Right to have their data deleted, anonymised or blocked if processed unlawfully, including data that does not need to be retained in relation to the purposes for which it was originally collected or subsequently processed.
• Right to receive a certification from the entities or individuals to whom the data was communicated that the above processes have been complied with (unless this requirement proves impossible or involves a manifestly disproportionate effort compared to the right that is to be protected).
• The right to object, in whole or in part, to the processing of their personal data:
-on legitimate grounds; or where the processing is carried out for the purpose of sending advertising materials or direct selling for the performance of market or commercial communication surveys.

9. FRANCE

- Under French Data Protection Law ("French DP Law"), purposes for processing personal data must also be determined, specific and legitimate.

- Under French DP law, personal data which is processed must be adequate, relevant and non-excessive in relation to the purposes for which it is processed.

- In addition to the right of access and correction, under French DP law, individuals benefit from the right of deletion and objection to the processing of their personal data upon legitimate grounds, as well as the right to give instructions as to the fate of the data subject's data after his/her death.

- Under French DP law, any automated processing must be notified to the French Data Protection Authority ("the CNIL") unless an official Data Protection Officer has been appointed according to French law specific requirements. In specific cases, such as in case of a data transfer outside of the EU, an authorization from the CNIL is also required.

- Under French DP law and according to the CNIL's guidance and case law, consent must be prior, explicit and specific (i.e. no consent is valid if given for several different purposes for instance). The consent must also be informed and freely given (i.e. no consent can be considered valid if the individual cannot refuse).

- Under French DP law, the use of personal data for a purpose which was not notified to the CNIL is unlawful.

- Under French DP law, additional data (not expressly designated as sensitive by the French DP Act) is also subject to specific requirements i.e. criminal offences and convictions, Social Security Number, biometric data and genetic dataa principle, the processing of sensitive data on employees is prohibited under French DP law. It may only be processed by the employer when specifically authorized by law.

- Under French DP law, data subjects must also be informed about the retention periods of their personal data or, if this is not possible, the criteria used to determine this period.

- Under French DP law, transfers of personal data outside the EU are subject to specific information requirements and individuals must be informed of the following elements: i) the list of countries outside of the EU where the data is transferred, ii) the categories of personal data that is transferred, iii) the purposes of the transfer, iv) the categories of recipients of the data transferred, and v) the safeguards implemented for ensuring an adequate level of protection to the transfer (i.e. EU standard contractual clauses, Privacy Shield for the US, Binding Corporate Rules).

- When personal data is collected through a form/questionnaire, the following information must be mentioned directly on the form: i) the identity of the data controller and of its representative, if any; ii) the purposes for which personal data is processed; iii) whether providing data is mandatory or optional and the possible consequences of the absence of a reply; and, iv) the data subject's rights of access, correction, deletion and objection to the processing of personal data upon legitimate grounds as well as the right to give instructions as to the fate of the data subject's data after his/her death.

- Such exemption does not apply under French DP law.

- Direct marketing communication to individuals via electronic means (i.e. emails, text messages) is subject to obtaining the individuals' consent for instance via a box to be ticked ("opt-in"). This does not apply to direct marketing communication between professionals, who must be offered a mean to object to the sending of such communication in each message ("opt-out").
  Direct marketing communication to individuals over the phone or by post requires to provide a mean to object to such communication ("opt-out"). In any case, all the mandatory information notice required by French DP law must be provided to the individual.

- Failure to comply with French DP law may lead to both administrative sanctions (up to 3,000,000 €) and criminal sanctions (up to 5 years of imprisonment and a fine up to 300,000 €).
- cannot be a valid ground for processing employees' data since, according to French Labour law and the CNIL's guidance, consent from an employee is not considered as freely givena principle, the collection of personal data on criminal offences and conviction is prohibited under French DP law.

- Under French DP law and Labour law, prior information and consultation of the Works Councils ("Comité d'entreprise" and "Comité d'hygiène, de sécurité et des conditions de travail") is mandatory in the following circumstances: i) the implementation of new technologies that may have an impact on the working conditions, and ii) the implementation of technologies which allow to monitor the employees (for instance: setting up of a CCTV system, recording of the phone conversations, using geo-tracking devices).

- If LUXOFT wishes to keep the CVs of unsuccessful applicants for future use, the relevant applicants must be informed of such processing, and should also give his/her consent according to the CNIL's guidance.

- In accordance with the CNIL's guidance, the collection of some information on job applicants is forbidden in France:

2. Date of entry into France, date of naturalization, modalities for the grant of French nationality and original nationality;
3. Social security number;
4. Details about military situation;
5. Former address;
6. Information about applicants' family (i.e. their name, nationality, job and employer);
7. Health status, size, weight, eyesight;
8. Housing conditions (owner or tenant);
9. Associative life;
10. Banking information, loans contracted, defaults on payments.

- French DP and Labour law, several requirements apply to the monitoring of employees including:

  Prior information and consultation of Works Councils ("Comité d'entreprise" and "Comité d'hygiène, de sécurité et des conditions de travail"), no approval required;

  Prior notification to the CNIL of the data processing relating to employee monitoring, except if a Data Protection Officer (DPO) has been appointed (in which case, the data processing must be mentioned in the DPO's register). In addition, if personal data is transferred outside of the EU, an authorization from the CNIL would be required;

  Prior notice to employees which should specify in particular the scope of the monitoring, its purposes, the recipients of the data collected and the data retention period.accordance with French Labour Law, the notice/policy on monitoring rules should be annexed to the Internal Ruling ("Règlement intérieur") to allow disciplinary sanctions against employees if they do not apply the rules on the use of IT systems.

- Under French law, emails received or sent by employees using their professional email address/account are presumed to be of a professional nature and may be thus accessed by the employer any time, without prior notice, including in the absence of the employee.

  The employer cannot access the employees' private emails (i.e. either because it is titled "private" or "personal" or because after the employer starts reading it appears that the content is private – then the employer should stop reading) without the consent or the presence of the employee. In order to be of the safe side, it is advisable to obtain a court order to be allowed to open a private email.

10. GERMANY

1. If Luxoft Germany has a works council, the implementation of the privacy policy could be subject to co-determination rights.

2. It is usually not permitted to collect criminal conviction data unless the job specifically requires it (e.g. financial crimes for a cashier).

3. Access to e-mails of employees marked as private / personal is generally not permissible. Emails which are clearly marked as personal or private may not be read or further processed. Personal use of LUXOFT GROUP's email systems is not permitted for German employees. Please be aware that the interception of emails which are not archived may constitute a criminal offence.

4. Before CCTV is introduced into areas which are not freely accessible to the public (including the car park and the reception area) you must seek guidance from the Data Protection Officer. German law on CCTV on company premises is subject to very strict rules and only permitted in very limited circumstances. Any kind of illegal monitoring is very sensitive in Germany and can lead to severe fines and a negative public image.

11. HONG KONG

II. LUXOFT GROUP should follow the Data Protection Principles which represents the core of the Ordinance covering the life cycle of a piece of personal data:

d) Personal data must be collected in a lawful and fair way, for a purpose directly related to a function /activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred.
e) Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used. A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.
f) Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.
g) A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.
h) A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.

III. Currently, there is no requirement for the registration of data users, to appoint a data protection officer, no restrictions for transfer of personal data outside of Hong Kong, no mandatory legal requirement for data users to notify authorities or data subjects about data breaches.

IV. A data user may collect personal data from data subjects if:

i) the personal data is related to a function of the data user
j) the collection is necessary, lawful and fair
k) the data collected is not excessive, and
l) the data user has been informed of the following:
m) whether the provision of personal data by data subjects is mandatory and the consequence(s) for not
n) supplying the data
o) the purposes for which the data will be used
p) the persons to whom the data may be transferred
q) the data subjects' right to request for access and/or correction their personal data, and
r) the contact details of the person to whom requests for access or correction should be sent.

V. Data users may not transfer personal data to third parties, unless the data subjects have been informed of the following before their personal data was collected:

s) that their personal data may be transferred
t) the classes of persons to whom the data may be transferred.

VI. The direct marketing provisions generally require data users who wish to either use or provide personal data for direct marketing purposes to make specific disclosures to the data subjects and obtain consents for such actions. The disclosures include:

u) a statement of intention to use/provide their personal data for direct marketing
v) a statement that the data user may not use/provide the personal data without the data subjects' consent
w) a dedicated channel via which the data subjects may give such consent
x) the kind(s) of personal data to be used/provided
y) the class(es) of persons to whom the personal data may be provided
z) the class(es) of goods/services to be direct marketed, and
aa) a statement that the personal data may be provided for gain, if applicable.

VII. Furthermore, if the consent was given orally, data users have the additional obligation to send a written confirmation to the data subject confirming the particulars of the consent received. In addition, when data users use personal data for the purposes of direct marketing for the first time, they must inform the subjects that they may opt-out at any time, free of charge.

12. LUXEMBOURG

1. The Luxembourg Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data (the "Data Protection Act") does not restrict the concept of 'personal data' to *living* individuals. Any information of any type regardless of the type of medium relating to an identified or identifiable natural person qualifies as personal data, regardless of whether this natural person is alive or deceased.

2. Pursuant to the Data Protection Act, there is no requirement of notification to the Luxembourg data protection authority (the National Commission for Data Protection) if:

    a. The data controller has designated a data protection officer, unless in case of processing for surveillance purposes. This exemption only applies if such data protection officer has been approved by the Luxembourg data protection authority;

    b. The processing of data – with the exclusion of sensitive data – takes place for HR management purposes, unless this data is used to assess the data subject.

3. The Data Protection Act also indicates genetic data as sensitive personal data. Moreover, data on offences, criminal convictions or security measures may only be processed in execution of a legal provision.

4. Under Luxembourg law, at least the information regarding the LUXOFT GROUP entity and the purposes for which the LUXOFT GROUP processes the personal data should be provided.

5. Please note that in certain instances, such as surveillance at the workplace, consent of the employee cannot constitute a legitimate condition for data processing by the employer.

6. The Luxembourg Criminal Records Act of 29 March 2013 explicitly allows the employer to request an employee or job applicant to produce an extract of his criminal record for the purposes of management and recruitment of staff. This extract, as well as the data contained therein, may not be kept for more than 2 years.

7. Pursuant to Article L. 261-1 of the the Luxembourg Employment Code, the employee must be notified that the monitoring will be carried out. Must also be notified: the joint company committee, the staff delegation or the Labour and Mines Inspectorate for employees falling within the scope of the legislation on private contracts and the employee representative bodies for the persons with a statutory employment status.

8. Please note that communications clearly marked as personal may not be read, even in exceptional circumstances where a problem relating to an employee’s excessive or unauthorised use is suspected.

9. The use of CCTV in the workplace is subject to prior authorisation by the Luxembourg data protection authority, unless only non-employees are monitored without recording. In the latter case, a notification with the Luxembourg data protection authority suffices.

13. MALAYSIA

a. In Malaysia, the Personal Data Protection Act 2010 ("PDPA") defines "personal data" as any information in respect of commercial transactions, which (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (ii) is recorded with the intention that it should be wholly or partly processed by means of such equipment; or (iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject. It does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010. The scope of protection is limited to personal data of living individuals and it does not include information about a dead individual nor does it cover other persons such as companies or businesses.

b. LUXOFT GROUP may not transfer the personal information of an individual to places outside Malaysia unless to such place as specified by the Minister, upon recommendation of the Commissioner, by notification published in the Gazette in which case the Minister may specify any place outside Malaysia if:

   a. there is in that place in force any law which is substantially similar to the PDPA, or that serves the same purposes as the PDPA; or
   b. that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA.

LUXOFT GROUP may transfer any personal data to a place outside Malaysia if:

- the individual consents to the transfer;
- the transfer is necessary for the performance of a contract between the individual and LUXOFT GROUP;
- the transfer is necessary for the conclusion or performance of a contract between LUXOFT GROUP and a third party which is entered into at the request of the individual or is in the interests of the individual;
- the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- LUXOFT GROUP has reasonable grounds for believing that in all circumstances of the case (i) the transfer is for the avoidance or mitigation of adverse action against the individual; (ii) it is not practicable to obtain the consent in writing of the individual to that transfer; and (iii) if it was practicable to obtain such consent, the individual would have given his consent;
- LUXOFT GROUP has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will – in that place – not be processed in any manner which, if that place was Malaysia, would be a contravention of the PDPA;
- the transfer is necessary to protect the vital interests of the individual; or
- the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

c. In Malaysia, there is no requirement to appoint a Data Protection Officer. However, a data subject must be given access to his personal data and has the right to correct it if it is inaccurate, incomplete, misleading or out-of-date. The data subject must make the request in writing and pay the prescribed fee to have a copy of his personal data. LUXOFT GROUP must comply with the request not later than 21 days or must inform why it is unable to comply within that period. LUXOFT GROUP must still comply no later than another 14 days after expiration of the first 21 days unless the following exceptions apply:

a. The data exporter may refuse to comply with a data access request within the prescribed 21 days period or a further 14 days period if:
   i. the data exporter is not supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the requestor;
   ii. the data exporter is not supplied with such information as he may reasonably require, where the requestor claims to be a relevant person, in order to satisfy himself as to the identity of the data subject in relation to whom the requestor claims to be the relevant person, and that the requestor is the relevant person in relation to the data subject;
   iii. the data exporter is not supplied with such information as he may reasonably require to locate the personal data;
   iv. the burden or expense of providing access is disproportionate to the risks to the data subject's privacy in relation to the personal data;
   v. the data exporter cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information unless that other individual has consented to the disclosure of the information to the requestor or it is reasonable in all circumstances to comply with the data access request without such consent;
   vi. any other data user controls the processing of the personal data in such a way as to prohibit the data exporter from complying, whether wholly or partly, with the data access request.

This, however, shall not operate so as to excuse the data exporter from complying with the data access request to any extent that the data exporter can comply with the request without contravening the prohibition;

vii. providing access would constitute a violation of an order of a court;
viii. providing access would disclose confidential commercial information; or
ix. such access to personal data is regulated by another law.

b. Separately, a data correction request need not be complied with if:

x. the data exporter is not supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the requestor;
xi. the data exporter is not supplied with such information as he may reasonably require, where the requestor claims to be a relevant person, in order to satisfy himself as to the identity of the data subject in relation to whom the requestor claims to be the relevant person, and that the requestor is the relevant person in relation to the data subject;
xii. the data exporter is not supplied with such information as he may reasonably require to ascertain in what way the personal data is inaccurate, incomplete, misleading or not up-to-date;
xiii. the data exporter is not satisfied that the personal data is inaccurate, incomplete, misleading or not up-to-date;
xiv. the data exporter is not satisfied that the correction is accurate, complete, not misleading or up-to-date; or
xv. any other data user controls the processing of the personal data in such a way as to prohibit the data exporter from complying, whether wholly or partly, with the data correction request. This, however, shall not operate so as to excuse the data exporter from complying with the data correction request to any extent that the data exporter can comply with the request without contravening the prohibition.

d. The PDPA is silent on whether an express or implied consent is required. The Personal Data Protection Regulations 2013 (“Regulations”), which stipulates that consent must be “recorded” and “maintained”, suggests that express consent is required. However recent proposal papers indicate that implied consent may be sufficient provided the individual has been made fully aware of the purposes of the processing of his personal data and as long as the data user is able to demonstrate that consent has been given by the individual.

e. Sensitive personal data also includes information as to the commission or alleged commission of any offence or any other personal data declared by the Minister to be sensitive personal data.

f. It is also necessary to provide any information available to LUXOFT GROUP about the source of that personal data, how to contact LUXOFT GROUP with any inquiries or complaints in respect of the personal data and the choices and means which LUXOFT GROUP offers the individuals for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data. Information provided must be in national and English languages.

g. According to the PDPA, this information should arguably be provided as there are no specific exceptions to the notice and choice principle which requires notice and disclosure for business contact information. However, in practice this is usually not observed. Notwithstanding the aforesaid, such business contact information may arguably be regarded as falling outside the definition of “personal data”. If the commercial transaction is between LUXOFT GROUP and a company, the personal data of representatives of the said company is arguably not “personal data” within the meaning of the PDPA as it is not in respect of commercial transactions that relate directly or indirectly to the representative (individual) of the said company. Therefore, such personal data might not be subject to the PDPA.

h. It is recommended that LUXOFT GROUP obtains consent from the employees when collecting normal personal data. However, the consent requirement is exempted for the performance of a contract to which the employee is a party. To qualify for exemption, LUXOFT GROUP must evaluate and determine what information is absolutely necessary for the discharge of the duties and obligations of both LUXOFT GROUP and the employee to avoid excessive data collection.

i. It is recommended that consent must be obtained from the unsuccessful applicants if LUXOFT GROUP needs to retain such personal data for other purposes including future use.

j. LUXOFT GROUP is not allowed to share data with third parties unless the consent of the employee is obtained.

k. Consent of the employees is required before sending direct marketing material to them. In addition, the employee must be given a right to refuse such use of their personal data at the time the data is collected using a free “opt-out” possibility.

l. LUXOFT GROUP is not allowed to disclose information about an employee for any purpose other than employment or to any third party other than the categories of people who will receive the data, of which the employee is fully aware and to which the employee has given consent. Nevertheless, personal data of the employee may be disclosed for any other purpose only under the following circumstances:

1. the employee has given his consent to the disclosure;
2. the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations;
3. the disclosure was required or authorized by or under any law or by the order of a court;
4. LUXOFT GROUP acted in the reasonable belief that it had a legal right to disclose the personal data to the other person;
5. LUXOFT GROUP acted in the reasonable belief that it the employee had given its consent if the employee had known of the disclosing of the personal data and the circumstances of such disclosure; or
6. the disclosure was justified as being in the public interest in the circumstances as determined by the Minister.

m. In Malaysia, LUXOFT GROUP can only install CCTV at workplace for the purpose of crime detection and prevention. It cannot be used for other purposes such as staff monitoring. Upon installation of CCTV, LUXOFT GROUP shall display a notice that is visible to visitors and place it at the entrance to the CCTV surveillance zone, informing them of the CCTV operation and the purposes for installation.

n. A third party service provider (“data processor”) who processes information on behalf of LUXOFT GROUP shall process such information only with the knowledge and authorisation of LUXOFT GROUP. LUXOFT GROUP shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor:

1. provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and
2. takes reasonable steps to ensure compliance with those measures.

o. There is no statutory retention period for the storage of CCTV images. It is recommended that the retention period should reflect the purpose of recording by LUXOFT GROUP. Images may be kept longer if needed for the purpose of investigation by law enforcement agencies. However, they must be deleted if there is no reason to keep them.

p. An individual’s image from the CCTV intended to be used by LUXOFT GROUP for the purposes agreed to by the individual must be clear, accurate and not misleading. LUXOFT GROUP may consider using suitable cameras depending on location and field of view to ensure images captured are of high quality, clear and precise. LUXOFT GROUP also has to ensure the same responsibility extends to any external processor LUXOFT GROUP intends to use for processing the CCTV footage.

q. Individuals have the right to view their own image captured upon their request. However, procedures for access along with necessary details from the individual should be provided explicitly by LUXOFT GROUP to confirm his/ her request for access to his/ her images only.

14. MEXICO

1. In Mexico a data subject also has the right to request that his personal data is deleted or cancelled (ARCO rights: the right to access, rectify or correct his data, cancel and oppose to certain types of processing). Cancellation of the personal data does not proceed automatically, therefore the specific situation has to be consulted with the Data Protection Officer to determine the course of action.

2. Under the Federal Law on the Protection of Personal Data held by Private Parties, there is no need for filings with the data protection authority.

3. The individual or data subject also has the right to request that his personal data is deleted or cancelled.

4. Even where consent is not required, the data subject must always be informed of the characteristics of processing of his data.

5. Use of data for a new purpose must always be informed to the data subject and in certain cases consent must also be requested.

6. Personal use of LUXOFT GROUP's email systems may be permitted as the client considers. However, if permitted, employees must be informed of the monitoring that may be carried out so that there is no expectation of privacy. Employees must be clear that email and other communications technologies are considered work tools subject to monitoring by the employer. The Data Protection Authority has not yet issued a resolution in this regard, where it clarifies if company email may or may not be accessed even when marked as personal. Please be aware that the interception of emails may constitute a criminal offence.

15. The Netherlands

1. Please note that in the Netherlands, photos and videos are also regarded as special personal data, and of a sensitive nature as they convey racial qualities of persons on the images. Because of this, the use of such personal data (i.e.. with CCTV and photo ID's on intranet) is subject to stricter rules.

2. If Luxoft Netherlands has a works council, the implementation of the privacy policy and any subsequent introduction of systems aimed at or capable of being used for monitoring the presence/absence, behaviour/conduct or performance of its personnel could be subject to co-determination rights, which may include prior consent from the works council.

3. Please note that due to the dependent relationship between employee and employer, consent given by employees is often not considered free.

4. The Dutch Data Protection Authority (**DPA**) states that employers are not allowed to access emails which are clearly marked as private. There might be some room for nuance in that statement, but it is advised to consult with a specialist or external counsel should Luxoft Netherlands wish to access private emails.

5. It is required to sufficiently address the matter of personal data breaches in a Data Processor Agreement, or any contractual clauses serving similar goals. It is also advised to include a section on Data Breaches in the specific Annexes for Sales, IT and Facilities to increase awareness.

16. POLAND

I. General information

1. Entity which collects personal data due to article 13 of GDPR is obliged to provide individuals whose personal data will be processed with the general information about the terms and conditions of processing of the personal data. In Poland this information typically is made in the form of written document.
2. Every time the information listed below specifies the obligations of the "employer" it means obligation of the LUXOFT entity which employs employees in regard to jurisdiction of polish legal system.
3. In Poland there are many obligations of the employer connected with processing of the personal data. Below there are listed only the most crucial ones.

II. Recruitment

1. Provisions of the polish Labour Code stipulate which personal data the employer is allowed to collect from the candidates, to process of which the consent of the candidate is not needed.
2. Current scope of personal data collected from candidates include*:

   b) Name and surname,
   c) Parents names,
   d) Date of birth,
   e) Address of residence,
   f) Education,
   g) Professional experience

   ** Abovementioned scope of the personal data is planned to be change due to implementation of the act exercising GDPR in Poland, which contains such changes as: right of the employer to obtain also information about special qualifications of the candidate, his/her contact information. On the other hand parents' names no more could be processed without the candidate consent.*

   Collected data should be used by the employer only to purposes of the specific recruitment process.

3. If candidate provide any additional personal data* (for example: his/her telephone number, e-mail address, salary expectations, notice period and others) – to process such data the employer should obtain explicit consent of the candidate.

   ** It should be noted that due to planned implementation of the act exercising GDPR in Poland, sensitive personal data about the candidate should not be processed even if he/she gives his explicit consent to such action. Due to that i*n Poland the employer can obtain information about the hypothetical employee's criminal convictions only if such right results directly from the specific legal provision.

   Additional consent is also required to process any personal data of the candidate to purposes of other recruitment processes. This consent should include information about the duration of the processing of the conferred personal data.

4. Personal data of the candidate can be processed until:

   a) finishing (successful or unsuccessful) of the specific recruitment process – if candidate did not give his/her consent to process such data for the purposes of other recruitment processes,
   b) finishing of the duration to which the candidate gives his/her consent to process such data for the purposes of other recruitment processes,
   c) the consent of candidate is revoked.

   In case of completion of the conditions described above all personal data of the candidate (CV, application forms, interview notes) which was used during the recruitment process should be deleted*.

   ** However the employer has a right to keep any information connected with the recruitment process if they may be needed due to hypothetical future court proceedings.*

III. Employment

1. The same regulations as described in point II above stipulate the scope of personal data that the employer can additionally obtain from the successful candidates (employees).
2. Current scope of personal data collected from the employees contains*:

   a) Data collected during the recruitment process:
      – Name and surname,
      – Parents names,

- Date of birth,
- Address of residence,
- Education,
- Professional experience

b) other personal data of the employee, if the provision of such data is necessary due to the employee's exercise of special rights provided in the Labor law;
c) the PESEL number of the employee.

**Abovementioned scope of personal data is planned to be changed, the new scope will include also information about the number of the identity card - in case the employee does not have the PESEL number.*

These data should be used by the employer only for the purposes of the employment contract.

3. In Poland the employer is also entitled to obtain other personal data of the employee only if such right results directly from other legal provisions (for example provisions which regulated the employer's obligation as a payer of taxes or social benefits). In case such right of the employer does not result from the legal provisions – the explicit consent of the employee is needed to legally process his/her personal data*.

** It should be noted that due to planned implementation of the act exercising GDPR in Poland, sensitive personal data about the employee should not be processed even if he/she gives his explicit consent to such action.*

To process any additional data of the employee, the employer needs to have his/her explicit consent for such action.

4. Personal data of the employee can be kept until:

a) employee's personnel file – ten (10) years from the termination of the employment agreement*,
b) Spent disciplinary convictions – one (1) year after of impeccable work,
c) Payroll and tax records – ten (10) years after the termination of the employment agreement,
d) Tax records – five (5) years from the end of the tax year in which the tax obligation arose.
e) Social benefits documents transfer to the Social Security Office – five (5) years from the date of transfer.

**Until 1st January 2019 the rule of keeping employee personnel file was fifty (50) years from the date of termination of the employment agreement.*

Due to established legal changes in the duration and method of keeping employee's personnel file this period now is shortened to ten (10) years.

Rules described below shall abide:

Date of establishing the employment relationship	Duration of storage	Description
before 1/01/1999	**50 years**	It is not possible to shorten the period of keeping employee documentation to 10 years. The **50-year** retention of documentation will continue to apply.
after 31/12/1998 and before 1/01/2019	**50 years / 10 years**	In the scope of these employment relationships, the provisions regarding the **50-year** period of storage of personal files and documentation applied. Under some circumstances the employer may shorten the period of storing employee documentation up to **10 years**. To take advantage of this opportunity employer is obliged to submit a statement to the Social Security Office about the intention to submit information reports* (ZUS OSW) and subsequently submit an information report (ZUS RIA). ***information report*** is a summary of information (income, working time, date of termination of employment and others) about the insured employee, necessary to determine the basis of the future retirement or pension. When this report will be submitted to Social Security Office, the period of storing the documentation will be **10 years**, counting from the end of the calendar year in which the information report was submitted.

		The report should be submitted for all employees employed from 1/01/1999 to 31/12/2018. It is not possible to submit a partial report for part of the employees and thus the storage of certain files for 10 years and some for 50 years.
after 31/12/2018	**10 years**	In the scope of these employment relationships, the employer is obliged to apply new regulations regarding the time of documentation storage. Documentation will be stored for a period of **10 years** from the end of the calendar year in which the employment relationship has been terminated or expired.

5. **Employee documentation**

- The employer can keep and store all documentation related to the employment relationship (employee documentation) in a chosen form - paper **OR** electronic.
- The form of keeping employee documentation may change during the employment relationship or after its completion.

Change of documentation form:

from paper to electronic:	from electronic to paper:
Making a digital copy of a paper document, in particular a scan, and then **applying it with a qualified electronic signature** or an authorized person, or a qualified electronic stamp of the employer confirming the compliance of the digital copy with a paper document.	Preparing a printout with a signature of the employer or a person authorized by him, confirming the compliance of the printout with the electronic document.

- The employer is obliged to inform employees and former employees about any change in the form of keeping records. The employee is entitled within 30 days from the date of obtaining of this information to collect the documentation in the previous form.

IV. Monitoring

1. Provisions of the Polish Labour Code stipulate conditions of implementation and maintenance of the video monitoring (CCTV), monitoring of the IT systems and business e-mail accounts.
2. Firstly the employer can implement video monitoring (CCTV) only if it's necessary to ensure safety of the employees or protection of property. The recordings from video monitoring (CCTV) shall be processed by the employer solely for the purposes for which they were collected.
3. As a rule video monitoring (CCTV):
   a) cannot violate the personal rights of the employees,
   b) cannot include: sanitary rooms, cloakrooms, canteens, smoking rooms or premises made available to the trade union organization.
4. The recordings from video monitoring (CCTV) shall be stored for a period not exceeding 3 months from the date of recording. However if such recordings are planned to be used as evidence during court proceedings – duration of storage of such recordings can be extended until the final conclusion of such proceedings. After the time specified in previous sentences the recordings containing personal data shall be destroyed.
5. Specific informational obligations burden the employer:
   a) to inform the employees about the implementation of the video monitoring (CCTV), every new employee shall be informed before he/she is admitted to work,
   b) to include information about the purposes, scope and method of monitoring in work regulations,
   c) to mark monitored premises with a visible and legible manner (sound and/or signs).
6. The employer is entitled to conduct monitoring of the IT systems and e-mail correspondence only if it is necessary to ensure the appropriate organization of working time and proper use of work tools.
7. Monitoring of the IT systems and e-mail correspondence should not violate the confidentiality of private correspondence and other personal rights of the employees.

V. Marketing

1. In Poland two other legal act concerns the issue of usage of the individual's personal data for the marketing purposes. These are:

Act on Telecommunications

The explicit consent of the end user of the telecommunications terminal equipment and automated calling systems is necessary to conduct any marketing actions.

Act on the providing of services by electronic means

It is forbidden to send unsolicited commercial information addressed to a designated recipient who is a natural person by means of electronic communication, in particular electronic mail. Commercial information is considered as ordered, if the recipient has consented to receive such information, in particular he has made available to him an electronic address identifying him/her.

2. Above means that even if the controller/processor identify other (than consent) legal basis of processing personal data of the individual for marketing purposes – in some cases it may still be obliged to obtain consent of such individual to provide him/her commercial information.

VI. Technical and organizational security measures

1. Every entity which process personal data (controller/processor) should take measures appropriate to secure the confidentiality of personal data being processed.
2. First step to secure personal data is to allow only persons who were granted authorization by the controller/processor to carry out data processing activities.
3. The controller/processor should keep a register of the persons authorised to carry out data processing, which should contain the following:
   i. full name of the authorised person,
   ii. date of granting and expiration, as well as the scope of authorisation to access personal data,
   iii. identifier, in cases where data are processed in an IT system,
4. The persons authorised to carry out the data processing shall be obliged to keep these personal data and the ways of their protection confidential.
5. A data controller/processor is obliged to keep and implement written documentation regarding data security principles.

The documentation may consist of: (1) the Security Policy and (2) instruction for using the data processing IT system (the "**IT Instruction**").

The Security Policy

The Security Policy should include in particular:

a) a list of buildings, premises or their parts comprising the area where the personal data are processed ('area were data are processed');
b) a list of data filing systems with an indication of software used for data processing. According to Polish law, a data filing system is a set of personal data that have a structure, is centralised or decentralised, and where data are available on the basis of at least one criterion);
c) a description of the structure of the data filing systems and indication of the content of particular information fields and connections between them;
d) method of transferring data between particular systems;
e) a definition of technical and organisational measures necessary to ensure confidentiality, integrity and accountability of the data being processed.

The instruction for managing the IT systems

The IT Instructions should consist of, in particular:

a) procedures for granting authorisation to process data by users (e.g. employees) and registration of these authorisations in the IT system, as well as indication of the person responsible for granting authorisations (e.g. *privacy officer/IT manager*);
b) methods and means of users' authorisation and procedures connected with the management and use of those methods and means;
c) procedures of beginning, suspending and terminating work by users of the IT system;
d) procedures of making backups of the data filing systems and programs and software tools used for the data processing (together with the location of backup copies);
e) method, place and period of storage of: (a) data carriers, and (b) backups referred to in point d);
f) method of securing the IT system against software serving for gaining unauthorised access to IT systems;
g) how the requirement is met that the IT system should allow for recoding of information on recipients to whom the data were disclosed and the date and scope of this disclosure;
h) procedures for inspecting and maintaining IT systems and data carriers used for personal data processing.

Specific obligatory security measures

Most controller/processors in Poland are obliged to apply a high level of security. The high level of security applies when the controller/processor uses an IT system that is connected to the Internet (at least by one device).

The following are minimum requirements in order to apply the high level of security:

a) Buildings, premises or their parts comprising the area where data are processed should be secured against access of unauthorised persons during the absence in this area of the persons authorised to process personal data.
b) Any unauthorised person may stay inside the area where the personal data are processed only upon the controller/processor's consent or in the presence of a person authorised to process personal data.
c) The mechanisms of access control should be applied in the IT system used for personal data processing.
d) A separate identifier should be registered for each IT system user.
e) Access to data should be available only after entering the identifier and the user's authentication.
f) The IT system used for personal data processing should be secured in particular against:
g) software used for gaining unauthorised access to the IT system;
h) loss of data which may be caused by any power supply failure or line interference.
i) The identifier of a user who has lost authorisation to personal data processing should not be granted to another person.
j) In the case where the password is used for user's authentication, the passwords should be changed at least once a month. In the case where the password is used for user authentication, the password should consist of at least eight characters, including small and capital letters, numbers and special characters.
k) Personal data being processed within the IT system should be secured by making back-ups of the data filing systems and using data processing software.
l) Back-ups should:
    i. be stored in the premises ensuring security against any unauthorised takeover, change, damage or destruction;
    ii. be deleted as soon as their usefulness ceases.
m) A person using a laptop containing personal data should be obliged to take special precautions while having the laptop transported, stored or used outside the area where data are processed, including cryptographic protection measures.
n) Devices, discs and other electronic information media containing personal data intended to:
    i. liquidation – should be devoid of those data, and in cases when it is impossible, the records should be damaged,
    ii. be turned over to any other party unauthorised to process personal data – should be devoid of the personal data,
    iii. be repaired – should be devoid of those data, thereby to make them not retrievable or should be repaired under supervision of a person who has been authorised.
o) The controller/processor should supervise the security measures to be implemented within the IT system.
p) Any devices and information media containing sensitive data being transferred outside the area where the personal data are processed should be secured in such a way to ensure confidentiality and integrity of these data – (according to the DPA, devices should be encrypted) (the IT instruction should cover the method of the application of this security measures).
q) The IT system used for personal data processing should be secured against any dangers originating from the Internet by the implementation of physical and logical security measures protecting against any unauthorised access (according to the DPA, personal data transferred via Internet should be encrypted).
r) In cases where the logical security measures referred to in point 15 are applied, these measures should cover:
    i. control of data flow between the IT system of the controller/processor and the Internet;
    ii. control of actions initiating from the Internet and the IT system of controller/processor.
s) The controller/processor should apply cryptographic protection measures for the data used for authentication which are being transferred within the Internet
t) IT systems used by the controller/processor to process personal data must also provide functionality that allows keeping a record of:
    i. the date when the personal data have been registered for the first time in the IT system,
    ii. an identifier of a user who registers the personal data in the IT system,
    iii. sources of personal data, if personal data have not been obtained from the data subject,
    iv. information on recipients ((i) to whom personal data have been disclosed and (ii) the date thereof and (iii) the scope of this disclosure),
    v. any objection of the data subject to process their data.

    This should be an automatic process. IT systems should save the data mentioned above after an authorised user enters data subjects' personal data to the IT system. Implementation and the whole process must be documented.

17. ROMANIA

1. Details about sickness can be recorded only if needed for compliance with the specific obligations of LUXOFT GROUP in labour field (e.g., for documenting the employees' absence).

2. Details of criminal offences should not be requested, unless such is legally requested for holding the respective position.

3. You must inform the unsuccessful applicants that you want to keep CVs on file for future use and CVs should only be retained if the applicants give their explicit consent on such.

4. Monitoring of employees' correspondence on a continuous basis (active monitoring) is not allowed. Likewise, monitoring/ processing of employees' e-mails clearly marked as "Private" or monitoring of employees' discussions by telephone or by way of other electronic communications means is strictly forbidden and may qualify as criminal offence.

5. The existence/ using of the CCTV needs to be pointed out by using a pictogram of an appropriate size and placed at a reasonable distance from the place where the CCTV cameras are installed. Generally, the use of CCTV within the area of the offices is strictly forbidden, save for the case where made based on the prior approval of the Romanian supervisory authority. Also, the use of hidden CCTV cameras is not allowed, unless in the limited cases set forth by the law. In no case may CCTV be used in places which, by their nature, impose the preservation of intimacy (e.g. toilettes).

18. RUSSIA

1. In Russia express consent of an employee in writing is necessary if the data is transferred to any third party and/or sensitive data (like religious beliefs) is collected and processed.

2. Processing information on criminal offences is prohibited except when the disclosure of this data is required by law for the purposes of employment.

3. In Russia an employee shall be aware about and give his/her written consent for any data transfers including those within or outside Russia.

4. The employer is prohibited from making decisions relating to employees based solely on data received automatically or electronically.

5. Sensitive information may be collected and processed only upon a written consent of the candidate; it is impossible to collect this information through the website.

6. The unsuccessful candidates should give their consent on the processing of personal data from their CV. Such consent can be granted in any form which can demonstrate that the consent is specified, well-informed and in full awareness. We recommend written form.

7. Background checks with third parties are allowed only upon written consent of the employee.

8. Written consent of a candidate shall be necessary for data transfers to the countries not providing an adequate protection for the personal data (i.e. having no unified law on a data protection and enforcement authorities).

9. In general monitoring of employee's e-mails and personal electronic activities may be interpreted as interference into private life or violation of secrecy of correspondence. Both constitute a criminal offense. Thus monitoring may not take place without express consent of an employee in writing.

19. SINGAPORE

1. "Personal data" under the Singapore Personal Data Protection Act 2012 ("PDPA") is defined as data, whether true or not, about an individual who can be identified from that data or from that data and other information to which an organisation has or is likely to have access. The data protection obligations under the PDPA do not apply to business contact information and the PDPA does not apply to personal data about deceased individuals except in relation to disclosure and protection of personal data of an individual who has been dead for 10 years or less. No consent is required for the collection, use or disclosure of personal data that is publicly available.

2. Generally, staff may only collect, use, disclose or otherwise process personal data for particular purposes where LUXOFT GROUP has first obtained consent for the collection, use or disclosure of the personal data for those purposes, unless exempted under the PDPA.

3. Under the PDPA, an organisation must not transfer any personal data to a country or territory outside Singapore unless it provides a standard of protection to the transferred personal data that is comparable to the protection under the PDPA.

4. LUXOFT GROUP has been provided with PDPA-compliant data transfer agreements to regulate the transfers of personal data out of Singapore.

5. Staff should seek the input of the Data Protection Officer if you are not sure whether a data transfer agreement is in place to facilitate the transfer of personal data out of Singapore to a third party or country.

6. New Uses: Under the PDPA, use of personal data for a new purpose will require fresh consent. Staff must therefore consult the Data Protection Officer if they wish to use personal data for a new purpose.

7. Access: Under the Singapore Personal Data Protection Regulations 2014, organisations must provide a written response to access and correction requests within 30 days. If an organisation cannot respond within 30 days, it must inform the individual in writing of when it expects to be able to respond to the request. Requests should therefore be forwarded promptly to the relevant persons responsible so that the organisation can comply with the statutory timeline.

8. The PDPA only imposes the retention and protection obligations on data processors, known as “data intermediaries” in Singapore. However additional obligations may be contractually imposed, as has been done in Supplementary Document 4. Supplementary Document 4 may be used to facilitate disclosures to third-party data intermediaries in Singapore with the appropriate changes (e.g. change references of the Directive to the Singapore Personal Data Protection Act, change references to the EEA to Singapore, etc.).

9. Transparency: There is no consent exception for visitors under the PDPA. We recommend that visitors are provided with purpose notification language prior to the Company collecting, using or disclosing their personal data when they visit the premises to obtain consent for stated purposes.

10. Retention: Under the PDPA, Luxoft must cease to retain personal data (i) as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for (ii) legal or (iii) business purposes. Therefore the 3 year period must be justifiable on one of the above three grounds.

20. SWEDEN

13. Under the Swedish Personal Data Act ("**PDA**") a data subject has the right to request access and to request the controller to correct, block or erase such personal data that has not been processed in accordance with Swedish law.

14. Under the PDA, the legitimate interest of the controller must outweigh the data subject's interest in protection against violation of his/her personal integrity.

15. When personal data is collected from a data subject, the information regarding the LUXOFT GROUP entity collecting the information shall contain the name of the LUXOFT entity (i.e. the name of the controller) and address.

16. Such request shall be made in writing and shall be signed by the applicant.

17. Processing of personal data in the workplace with consent as legal ground shall be limited to situations where the employee is provided with a de facto choice of whether he/she should accept the processing or not and where the employee at a later stage may withdraw his/her consent without facing any negative consequences.

18. In general it is prohibited for others than public authorities to process personal data concerning legal offences involving criminal offences, judgments in criminal cases, coercive criminal procedural measures or administrative deprivation of liberty, even under circumstances where consent is obtained from the data subject. There are, however, exemptions to this prohibition; e.g. a controller may process such personal data concerning a data subject if (i) the processing relates to a single item of information which is necessary for the controller to process in order to determine, enforce or defend claims in an individual case or (ii) it is necessary for the compliance with a statutory notification requirement.

19. If LUXOFT GROUP wishes to keep the data for future recruitment needs, the candidate must be informed about this and give his/her consent.

20. It is generally not permitted to access employees' e-mails marked as private/personal. However, exceptions may apply when a serious suspicion of disloyal or criminal behaviour or a serious suspicion that the employee uses the IT equipment in violation of the employer's rules and guidelines exists.

21. The PDA does not impose requirements for implementation of specific security measures. The PDA only states that the controller shall implement appropriate technical and organisational measures to protect the personal data processed. Consequently, the controller needs to conduct an impact assessment in order to determine the appropriate level of protection. The measures taken shall provide a level of security that is appropriate having regard to (i) the technical possibilities available, (ii) what it would cost to implement the measures, (iii) the special risks that exist with processing personal data and (iv) the sensitivity of the personal data processed.

22. Before CCTV is introduced in a non-public area or in a public area you shall seek guidance from the relevant Data Protection Officer. The use of CCTV in non-public areas (e.g. in an office) (and in a public area) is subject to specific rules in the Swedish Camera Monitoring Act (2013:460) and the Swedish Camera Monitoring Ordinance (2013:463) and is only permitted under certain circumstances.

23. No specific maximum/minimum retention period applies for visitor registers, i.e. such records may not be kept for a longer period in time than is necessary having regard to the purpose of the processing. Consequently, the three (3) year period has to be justified with regard to the purpose of the processing.

21. SWITZERLAND

1. Under Swiss law, personal data includes all information that relates (either directly or indirectly) to an identified or identifiable individual or legal person (corporate entity). Foreign countries do not offer an adequate level of legal protection for personal data related to a legal person. The Swiss-US Safe Harbor scheme and the standard contractual clauses provided by the EU Commission do not include personal data related to a legal person. Additional protections for personal data may be necessary, as an amendment of the standard clauses.

2. Information shall be provided if sensitive data is collected.

3. It is usually not permitted to collect criminal conviction data unless the job specifically requires it (e.g. financial crimes for a cashier).

4. The unsuccessful applicant shall consent.

5. General monitoring of an employee's behaviour is not permissible (e.g. permanent monitoring of an employee's e-mail correspondence on a non-anonymous basis). With respect to the monitoring of the internet and/or e-mail use, permanent monitoring is permissible if such monitoring is based on anonymized log files (monitoring on a non-personal basis). Once a misuse has been discovered, the employer may then analyse the log file on a personal basis. In addition, the log files may be analysed on a personal basis if there are specific indications that there has been a breach of the rules by an employee. In any event, for such monitoring to be permissible, the respective employer must implement a monitoring policy which must be disclosed to the employees. Representatives of employees shall be consulted before the adoption of the policy.

6. The access to any e-mails clearly marked as private is prohibited and may even constitute a criminal offence.

7. Reference to the Federal Data Protection Act to be added.

22. UK

1. 'Personal data' is defined under the Data Protection Act 1998 ("Act") or General Data Protection Regulation (GDPR) as data relating to living individuals who can be identified from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2. Data controllers who process personal data must inform the Information Commissioner so that their processing of personal data may be registered and made public in the register of data controllers, unless an exemption applies.
   The registration is made via a simple online form and must include following descriptions:
   - what data is being collected and why it will be processed
   - the categories of data subject data is collected from
   - whether the data will be transferred either within or outside the European Economic Area.

   Data controllers can also provide their own specific descriptions.
   There is no requirement in the UK for organizations to appoint a data protection officer, unless you are:
   - Public authority;
   - The nature of processing activities requires the appointment of a DPO;
   - DPO was appointed base on professional qualities and expert knowledge of data protection law and practices;
   - DPO appointed voluntarily.

   Data controllers may collect and process personal data when any of the following conditions are met:
   - the data subject consents
   - the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party
   - the processing satisfies the data controller's legal obligation
   - the processing protects the data controller's vital interests
   - the processing is required by an enactment, the Crown or the government
   - the processing is required to perform a public function in the public interest, or to administer justice
   - the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests.

   Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions.

3. The data controller must provide the data subject with fair processing information about the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.
   Data controllers may transfer personal data out of the European Economic Area if any of the following conditions are met:
   - the data subject consents.
   - the transfer is essential to a contract to which the data subject is party.
   - the transfer is needed to carry out a contract between the data controller and a third party if the contract serves the data subject's interests.
   - the transfer is legally required or essential to an important public interest.
   - the transfer protects the data subject's vital interests
   - the data is public

4. Transfers of personal data to jurisdictions outside of the European Economic Area are allowed if the jurisdiction provides 'adequate protection' for the security of the data, or if the transfer is covered by 'standard contractual clauses' approved by the European Commission, or subject to an organization's Binding Corporate Rules. There is no requirement in the UK to notify the ICO of the use of the standard contractual clauses or to file these with the ICO.

5. For transfer of data to the United States, compliance with the US - EU Privacy Shield framework can satisfy the requirements of the UK's transfer restrictions.

6. The Act does not specify specific security measures to adopt and implement by data controllers.

7. There is a requirement to report a breach to the ICO within 72 hours of becoming aware, if there is a high risk of adversely affecting individuals rights and freedoms. A record of any personal data breaches must be kept of whether Company is required to notify.

8. None contained in the Act. However, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PEC Regulations') require providers of a public electronic communications service to notify the ICO (and in some

cases subscribers) in the event of a personal data breach. Failure to comply with an enforcement notice from ICO is a criminal offence.

9. Financial services firms regulated by the Financial Conduct Authority (FCA) may find that a breach of the Act may also give rise to enforcement action by the FCA in respect of a breach of the FCA Principles for Business.

10. The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data for direct marketing purposes.

11. The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.

23. UKRAINE

1. It was mandatory for companies to register databases containing personal data until 2014. Since 8 January 2014, companies are only required to notify the Ombudsman on the processing of personal data which are of particular risk to the rights and freedoms of an individual (pertaining to sensitive information or the so called 'risky data').

   At the beginning of this year 2014 the Ukrainian Parliament Commissioner for Human Rights (the Ombudsman) became the new regulatory authority. Having approved a new privacy compliance audit procedure, the Ombudsman is now authorised to perform data compliance audits. The privacy compliance audit procedure contains the rules governing audits and describes the types of the audits that may be undertaken (such as on-site or internal, scheduled or unscheduled). Following an audit, the Ombudsman or its authorised representative can issue an order for privacy compliance. This order is binding and failing to comply will give rise to liability.

2. According to the local legislation, 'risky data' includes data on: race, ethnic and national origin; political, religious or ideology beliefs; membership in political parties, trade unions, religious organizations or ideology NGOs; health; sexual life; biometrical data; genetic data; administrative or criminal liability records; criminal prosecution and police investigation measures; being victim of certain violence; personal location.

   When processing any categories of 'risky data', the data controller must notify the Ombudsman within 30 days from the date of starting the processing of such data. Notification may be carried out in different ways (e.g. by letter, e-mail, fax, etc.) and the Ombudsman has approved notification templates to streamline the procedure for data controllers. Companies that process 'risky data' about their employees (e.g. health records, temporary disability information) may be exempted from the notification procedures if that data is processed for employment purposes only.

3. Only information about the Personal Department responsible for protection of personal data relating to 'risky data' must be notified to the Ombudsman.

4. If you collect personal data about individuals, you must provide also the following information: name of LUXOFT entity and its location.

5. In Ukraine, when the LUXOFT GROUP collects personal information from an individual, it must also inform the individual of the location where the personal data are/will be kept.

6. According to the legislation of Ukraine, violation of personal data protection legislation is subject to an administrative liability. No criminal liability is prescribed by the law.

7. LUXOFT GROUP is entitled to process information about an individual without his/her consent when it is necessary to protect his/her vital interests, but up to the date when obtaining consent becomes possible. It is also recommendable to obtain consent for processing the data of job applicants.

8. Processing of information on criminal offence of an individual is a subject to notification the Ombudsman within 30 days from the date of starting the processing.

9. Use of data for a new purpose must always be informed to the individual and in certain cases consent must also be requested.

10. You must inform the unsuccessful applicants that you want to keep CVs on file for future use and CVs should only be retained if the applicants give their explicit consent on such.

24. USA

1. There are strict limitations regarding the use of criminal background checks, which vary by state and even down to local city ordinances. Before applicants are requested to provide such information, legal advice must be obtained for the specific request.

2. Generally notice is not required under U.S. law.

3. An employee in the U.S. is not required to explicitly consent to the gathering of their personal data for employment purposes.

4. Employees should be told clearly whether their electronic communications will be monitored and how.

5. Retention of HR records in the United States is governed by both federal (FED) and state law. Luxoft offices located in California Connecticut, Illinois, Indiana, Michigan, New Jersey, New York, North Carolina, South Carolina, Tennessee, Texas and Washington may have different statutory requirements as indicated in this matrix. In some instances there were several laws within the same jurisdiction that imposed different record retention periods; in this case we used the longest period in the matrix. If the state and federal retention periods differ, employer must comply with the jurisdiction that requires the longest retention period. This matrix does not include local city ordinances that may apply. For example, New York City and San Francisco city may have different retention periods.

6. Effective January 1, 2020, the California Consumer Privacy Act (CCPA) introduces new data privacy rights for California residents.

25. VIETNAM

1. LUXOFT GROUP may only process personal data where it has a lawful purpose for this and after obtaining prior consent from the relevant individual (in Vietnam: “data owner”).

2. Generally, staff may collect and process personal data (1) after consent from the relevant individual (in Vietnam: “data owner”) has been given and (2) process the personal data for the purposes and store it only for a given period of time as agreed by the relevant individual.

3. In addition, LUXOFT GROUP must provide information about the form, scope, place and period for storing the information.

4. In addition to accessing and correcting, Vietnam law allows individuals to cancel (i.e. delete) their personal information which is stored on a network.

5. In Vietnam, LUXOFT GROUP should not process information about applicants and employees without their consent.

6. Where LUXOFT GROUP provides staff data to third parties to provide benefits, make staff aware of this in the literature used to explain the benefits (e.g. pension, insurance or private health providers) and ensure that consent from each employee has been provided. If LUXOFT GROUP collects information to pass on to the third parties for whatever purpose, do ensure that consent from each employee has been obtained.

7. References: always check with the employee and ensure that his/her consent has been obtained before providing a reference.

8. The Head of Personnel Department must authorise any requests to monitor specific employees. This would apply to any of monitoring IT Equipment and traffic on the IT Network telephone calls and other forms of monitoring. Before authorising any monitoring, the Head of Personnel Department shall – in addition to the other requirements listed – ensure that consent from such employee has been obtained.

26. KOREA

1. The Personal Information Protection Act defines personal data as personal information pertaining to any living person that makes it possible to identify such individual by their name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information).

- 2. Sensitive Data means any information that, if divulged, may considerably infringe on the data subject's privacy, such as information related to an individual's ideology, faith, labour union membership, political views, affiliations with a political party, health or medical treatment, sexual orientation, genetic profile, criminal records and include any other information listed in a relevant executive ordinance. Particular Identification Data (or “Direct Personal Data”) means resident registration numbers (RRNs), passport numbers, driver's licence numbers and alien registration numbers. Consent to the processing of particular identification data and sensitive data must be obtained from the data subject separately from each other and from any other type of consent. There is a prohibition against processing of RRN by data handler unless the processing of RRNs is specifically required or permitted by a law or regulation, or there is a clear and urgent need to protect the life, body or economic interest of the data subject or a third party, or the processing of RRNs is unavoidable in the cases prescribed by decree of the Ministry of Interior and Safety.

- 3. The Personal Information Protection Act does not distinguish between Data Controllers or Data Processors. Both are considered to be “Personal information processor" which means a public institution, legal person, organization, individual, etc. that processes directly or indirectly personal information to operate personal information files for official or business purposes.

- 4. There is no specific exception to applicability that relates to publicly available information.

- 5. A data protection agreement must be in place between the Personal information processor in the context of any outsourcing. This requirement applies also to international personal information transfers. The Personal information processor must also inform data subjects when the Personal information processor provides personal information to a third party overseas, and the Personal information processor shall not enter into a contract for unlawful cross-border transfer when it obtains consent.

27. CHINA

1. Personal Information - “information recorded in electronic form or otherwise, and used independently or in combination with other information to make a natural person identifiable, including the name, date of birth, ID number, personal biological identification information, address, and telephone number of the natural person.”

2. Personal sensitive information means “information closely related to personal interests, including ID card number, finger print, gene, bank account, communication record, property information, credit information, trace track, trading information etc., and whose disclosure/abuse may damage personal safety, property safety, personal reputation, personal mental health, or lead to discriminatory treatment.”

3. “Network” means the system that consists of computers or other information terminals and related equipment for collecting, storing, transmitting, exchanging, and processing information according to certain rules and procedures.
4. “Network operator” means the owners and administrators of the network as well as network service providers.
5. Network operators are prohibited from collecting personal data that is not relevant to the services they offer. It is not known how strictly this prohibition will be enforced.
6. Before collecting personal data from an individual (the Data subject), a network operator is required to explicitly inform the individual of the purposes, means and scope of the collection and use of their data, and obtain their consent for collection. Any processing of personal data must be done in accordance within the scope of those consents. Informed consent of Data subjects to transfer or disclose any of its personal data to a third party (whether within or outside the country).
7. For overseas transfer of personal data, the network operator must first notify the Data Subject of:

    - type of personal data being transferred (it is unclear how much detail must be given);
    - purpose and scope of the transfer;
    - recipient and the country to which the data will be transferred;

8. Network operators are also required to back up and encrypt ‘important data’, and to store operations logs for at least six months. The Security Assessment Measures define ‘important data’ as data that is closely related to national security, economic development and societal and public interests (there is no definition in the Cyber Security Law itself).