

Polityka Bezpieczeństwa

dotycząca zbiorów danych osobowych
administrowanych przez Luxoft Poland sp. z o. o.
z siedzibą w Zabierzowie

§ 1.**Postanowienia ogólne**

1. Luxoft Poland sp. z o. o. działając w wykonaniu obowiązku wynikającego z § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych ustanawia niniejszą Politykę Bezpieczeństwa Luxoft Poland sp. z o.o. zwaną dalej „Polityką Bezpieczeństwa”.
2. Celem niniejszej Polityki Bezpieczeństwa jest zapewnienie możliwie jak najwyższego standardu prowadzonej przez Spółkę działalności gospodarczej przy jednoczesnym poszanowaniu obowiązków ciążących na Spółce z mocy obowiązującego prawa.
3. Polityka Bezpieczeństwa odnosi się do bezpieczeństwa informacji przechowywanych w zbiorach danych osobowych wymienionych w rejestrze zbiorów danych prowadzonym przez administratora bezpieczeństwa informacji powołanego przez Spółkę.

§ 2.**Definicje**

Ileć w Polityce Bezpieczeństwa występują wymienione poniżej wyrażenia, należy rozumieć je

Security Policy

concerning personal data filing systems
administered by Luxoft Poland sp. z o. o.
with a registered office in Zabierzów

§ 1.**General Provisions**

1. Luxoft Poland sp. z o. o. establishes the present Security Policy acting in performance of the obligation resulting from § 3 of the regulation of Minister of the Interior and Administration issued on April 29th, 2004 concerning documentation of processing of personal data and the technical conditions which must be fulfilled by the equipment and IT systems used to process the personal data.
2. The purpose of the present Security Policy is to ensure the highest possible standard of the Company's business activity conducted with a respect to the obligations binding on the Company under the applicable law.
3. The Security Policy concerns the security of information stored in the personal data filing system mentioned in the register maintained by information security administrator appointed by the Company.

§ 2.**Definitions**

The defined terms mentioned in the present Security Policy shall be understood in a

następująco:

1. **Administrator Danych** - Luxoft Poland sp. z o.o. z siedzibą w Zabierzowie, adres ul. Krakowska 280, 32 – 080 Zabierzów, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie XII Wydział Gospodarczy KRS pod numerem KRS 0000359814, posiadającą kapitał zakładowy w wysokości 650.000 zł, REGON 121272822, NIP 676-242-31-85,
2. **bezpieczeństwo informacji** – kompletność i dokładność danych znajdujących się w zbiorze danych oraz metod ich przetwarzania, utrzymanie dostępu do danych oraz związanych z nimi aktywów jedynie dla osób upoważnionych i jedynie w wypadkach, gdy istnieje taka potrzeba. Bezpieczeństwo informacji jest podstawowym mechanizmem umożliwiającym współużytkowanie informacji.
3. **Instrukcja Zarządzania Systemem** – dokument wydany przez Administratora danych dotyczący zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji
4. **Polityka Bezpieczeństwa** – niniejsza Politykę Bezpieczeństwa Zbiorów Danych administrowanych przez Luxoft Poland sp. z o.o. z siedzibą w Zabierzowie
5. **Zbiór danych** - zbiór danych wpisany do rejestru, o którym mowa w § 1 ust. 3 Polityki Bezpieczeństwa.

following way:

1. **Controller** - Luxoft Poland sp. z o.o., a limited liability company with its registered office in Zabierzów, ul. Krakowska 280, 32 – 080 Zabierzów, registered under the number KRS 0000359814 in the Register of Entrepreneurs of the National Court Register with the District Court for Kraków-Śródmieście in Kraków, XII Commercial Division of the National Court Register, with a share capital of PLN 650,000, REGON (Industry ID Number) 121272822, NIP (Tax Reg. No.) 676-242-31-85
2. **Information security** – completeness and accuracy of the data stored in a filing system as well as completeness and accuracy of the processing methods, maintaining access to data and to related assets only for the authorized persons and only when it is necessary. The information security is a fundamental mechanism that enables the information sharing.
3. **The System Security Instruction** – a document issued by the Controller concerning the management of IT system used to process the personal data with a special respect of the data protection requirements
4. **Security Policy** – the present Security Policy concerning personal data filing systems administered by Luxoft Poland sp. z o.o. with a registered office in Zabierzów
5. **Filing system** – a filing system entered into the register mentioned in § 1 section 3 of the Security Policy.

§ 3.**Obszar, w którym przetwarzane są dane**

Obszarem przetwarzania danych są biura Administratora Danych, znajdujące się w następujących lokalizacjach:

- Quattro Business Park, ul. Bora Komorowskiego 25D, 31-476 Kraków
- Kraków Biznes Park. ul. Krakowska 280, 32 – 080 Zabierzów
- Silver Tower, Pl. Konstytucji 3 Maja 3, 50-083 Wrocław
- Green Day, ul. Szczytnicka 9, 50-382 Wrocław
- Olivia Business Centre, al. Grunwaldzka 472A, 80-309 Gdańsk

§ 3.**The area where the data are processed**

The area where the data are processed are the Controller's offices which are in following locations:

- Quattro Business Park, ul. Bora Komorowskiego 25D, 31-476 Kraków
- Kraków Biznes Park. ul. Krakowska 280, 32 – 080 Zabierzów
- Silver Tower, Pl. Konstytucji 3 Maja 3, 50-083 Wrocław
- Green Day, ul. Szczytnicka 9, 50-382 Wrocław
- Olivia Business Centre, al. Grunwaldzka 472A, 80-309 Gdańsk

§ 4.**Zbiory danych osobowych i programy stosowane do ich przetwarzania**

Administrator Danych prowadzi następujące zbiory danych osobowych:

1. Zbiory w formie papierowej:
 - a. Zbiór danych osobowych pracowników Luxoft Poland sp. z o. o.
 - b. Zbiór danych osobowych osób fizycznych nieprowadzących działalności gospodarczej, wykonujących czynności na rzecz Luxoft Poland sp. z o.o. na podstawie zawartych umów,
 - c. Zbiór danych osobowych osób fizycznych prowadzących działalność gospodarczą i świadczą usługi na rzecz Luxoft Poland sp. z o. o. na

§ 4.**Personal data filing systems and the software used to process the data**

The Controller conducts the following personal data filing systems:

1. The paper supported filing systems:
 - a. The filing system which contains the data of employees of Luxoft Poland sp. z o. o.
 - b. The filing system that contains the data of physical persons who do not conduct the business activity and who perform the services to Luxoft Poland sp. z o. o. under the executed contracts
 - c. The filing system that contains the data of the physical persons who conduct the business activity and who perform the services to Luxoft Poland sp. z o. o.

podstawie zawartych umów

under the executed contracts.

2. Zbiory w formie elektronicznej:

- a. Zbiór danych osobowych kandydatów na pracowników oraz pracowników obsługiwany przez program LuxStaff
- b. Zbiór danych osobowych pracowników Luxoft Poland sp. z o. o. obsługiwany przez program Xpertis
- c. Zbiór danych osobowych pracowników oraz kontrahentów Luxoft Poland sp. z o. o. na potrzeby księgowości.

2. The electronic supported filing systems:

- a. The filing system that contains the data of the candidates for employees as well as the data of employees supported by Lux Staff program.
- b. The filing system that contains the data of employees of Luxoft Poland sp. z o. o. which is supported by Xpertis program.
- c. The filing system that contains the personal data of employees and the contractors of Luxoft Poland sp. z o. o. for the purposes of accounting

Dane osobowe przetwarzane są w zbiorach danych obsługiwanych przez następujące programy:

- HR Xpertis,
- aplikację internetową Lux Staff,
- Oracle
- Symfonia

The personal data are processed in filing systems supported by the following programs:

- HR Xpertis,
- Internet application Lux Staff,
- Oracle
- Symfonia

Wszystkie wyżej wymienione programy działają w ramach systemu informatycznego Luxoft Poland sp. z o. o. W systemie informatycznym stosuje się wysoki poziom bezpieczeństwa w rozumieniu rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Z 2004 r. Nr 100 poz. 1024).

All the above mentioned programs work operate within the IT system of Luxoft Poland sp. z o. o. The computer system uses the high level of security as defined by the regulation of Minister of the Interior and Administration issued on April 29th, 2004 concerning documentation of processing of personal data and the technical conditions which must be fulfilled by the equipment and IT systems used to process the personal data. (Law Journal of 2004, n° 100 section 1024).

§ 5.

Struktura zbiorów danych osobowych

Zbiory danych osobowych zawierają następujące dane:

1. Zbiory w formie papierowej:

- a. Zbiór wskazany w § 4 ust. 1 lit. a odpowiada prawnie regulowanej strukturze akt osobowych pracownika to jest:

Część A: imię, nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania, wykształcenie, przebieg dotychczasowego zatrudnienia.

Część B: stanowisko, miejsce pracy, wysokość wynagrodzenia, termin rozpoczęcia pracy, czas trwania umowy o pracę,

Część C: data zakończenia umowy o pracę, ewentualnie wysokość ekwiwalentu za niewykorzystany urlop.

- b. Zbiór wskazany w § 4 ust. 1 lit. b

Imię, nazwisko, adres zamieszkania, numer PESEL, wysokość wynagrodzenia, numer rachunku bankowego.

- c. Zbiór wskazany w § 4 ust. 1 lit. c

Imię, nazwisko, adres zamieszkania, numer PESEL, wysokość wynagrodzenia, numer rachunku bankowego

2. Zbiory w formie elektronicznej:

- a. Zbiór wskazany w § 4 ust. 2 lit. a

Imię, nazwisko, stanowisko, projekt do obsługi, typ zatrudnienia, poziom zaszeregowania, wymiar czasu pracy, jeśli pracownik podjął pracę w wyniku transferu z innej spółki grupy Luxoft – wskazanie tej spółki

§ 5.

The structure of the personal data filing system

The personal data filing systems contain the following data:

1. The paper supported filing systems:

- a. the filing system mentioned in § 4 section 1 point a complies with the legal requirements applicable for the employees' personal files:

Part A: name, surname, the parent's names, date of birth, domicile, education background,

Part B: position, the work place, salary, the work contract duration

Part C: the work contract termination date, the amount of compensation for an unused employee's leave

- b. the filing system mentioned in § 4 section 1 point b

Name, surname, domicile, PESEL number, the salary amount, the bank account number.

- c. the filing system mentioned in § 4 section 1 point c

Name, surname, domicile, PESEL number, the salary amount, the bank account number.

2. The electronic supported filing systems:

- a. the filing system mentioned in § 4 section 2 point a

Name, surname, supported project, the employment type, grade, working hours, if the employee was transferred from another company of Luxoft group, the name of the

b. Zbiór wskazany w § 4 ust. 2 lit. b

Numer teczki (unikatowy numer nadany pracownikowi), imię, nazwisko, jednostka organizacyjna w której pracownik wykonuje obowiązki, charakter pracy (pracownik fizyczny lub umysłowy), typ umowy o pracę, podległość służbowa, okresy zatrudnienia u innych pracodawców, wykształcenie, okresy nieobecności w pracy, urząd skarbowy, z którym rozlicza się pracownik, adres pracownika, numer rachunku bankowego pracownika.

c. Zbiór wskazany w § 4 ust. 2 lit. c

Imię, nazwisko, numer rachunku bankowego.

§ 6.**Przepływ danych między systemami**

Dane znajdujące się w zbiorach danych osobowych wskazanych w § 4 ust. 1 podawane są przez osoby, których dane dotyczą.

Dane znajdujące się w zbiorach danych osobowych wskazanych w § 4 ust. 2 lit. a i b wprowadzane są przez pracowników Administratora Danych za pomocą terminali komputerowych znajdujących się w lokalizacjach wymienionych w § 3 Polityki Bezpieczeństwa na podstawie danych zgromadzonych w zbiorach danych wskazanych w § 4.

§ 7.**Środki techniczne i organizacyjne używane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych**

1. Na czas nieobecności osób upoważnionych do przetwarzania danych osobowych w

company

b. the filing system mentioned in § 4 section 2 point b

File number (unique number assigned to an employee), name, surname, business entity where the employee works, work character (mental work or physical work), the employment agreement type, subordination, the employment periods in other companies, educational background, the absence from work periods, the employee's tax office, domicile, the bank account number

c. the filing system mentioned in § 4 section 2 point c

Name, surname, the bank account number.

§ 6.**The data transfer between the systems**

The data stored in the filing systems mentioned in § 4 section 1 are supplied by the persons who are the subjects of the data.

The data stored in the filing systems mentioned in § 4 section 2 point a and b are entered into the filing system by the Controller's employees via computer terminals situated in the locations mentioned in § 3 of the Security Policy. The data are entered on the base of the data stored in the filing systems mentioned in § 4.

§ 7.**The technical and organizational means used to ensure confidentiality, integrity and accountability of the data processing**

1. The area where the personal data are processed data in the filing system is

obszarze przetwarzania danych w ramach zbioru danych, zabezpiecza się go przed dostępem osób nieuprawnionych. Biuro Administratora Danych monitorowane jest przez służby ochrony przez całą dobę.

protected while the persons authorized to process the personal are not present there. The Controller's office is monitored around the clock by the security service.

2. Urządzenia służące do przetwarzania danych osobowych znajdują się w strefie kontrolowanego dostępu, do której prawo wejścia mają pracownicy Administratora Danych. Dostęp do pomieszczeń jest kontrolowany za pomocą kart magnetycznych wydawanych osobom uprawnionym. Osoba przykładając kartę do czytnika znajdującego się przy wejściu do budynku, w którym znajduje się biuro oraz do czytnika, który znajduje się przy wejściu do biura położonego na określonym piętrze budynku.
2. The equipment used to process the personal data is situated in a zone of controlled access which can be entered just by the Controller's employees. The access is controlled by the use of magnetic cards which issued to eligible persons. A person puts the card into a reader which is situated at the entrance of the office building as well as at the entrance to the office on a particular floor of the office building.
3. W zakresie niezbędnym do zabezpieczenia danych i do uniknięcia wycieku danych ze zbiorów danych osobowych stosuje się niszczarki dokumentów. Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich nieprzydatności niszczone natychmiast.
3. The shredders are used as quickly as it is necessary to protect the data and to avoid data leak from the personal data filing system. Temporary printouts containing the personal data are destroyed as soon as their unsuitability is discovered.
4. Osoby nieuprawnione do przetwarzania danych, o których mowa w ust. 1 mogą przebywać w obszarze ich przetwarzania jedynie za zgodą Administratora Danych oraz jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych przez Administratora Danych.
4. Persons who are not authorized to process the data mentioned in section 1 can stay in the area where the data are processed only with consent of the Controller and only in presence of the person authorized by the Controller to process the personal data.
5. Dostęp do danych osobowych znajdujących się w zbiorze danych podlega kontroli poprzez przyporządkowanie osobom upoważnionym do przetwarzania danych osobowych identyfikatora oraz hasła na zasadach przewidzianych w Instrukcji Zarządzania
5. The access to the personal data stored in a filing system is controlled by the use of an ID assigned to a person authorized by the Controller to process the personal data as well as by granting to this person a password under the rules set forth in the System Security Instruction.

- Systemem.
6. Pracownicy mają dostęp do aplikacji zawierających dane osobowe związane z wykonywaniem ich obowiązków służbowych.
 7. Pracownicy przetwarzający dane osobowe zobowiązani są do zachowania ich w tajemnicy na podstawie umów o obowiązku zachowaniapoufnościawartychz Administratorem Danych. Osoby te są przed dopuszczeniem ich do przetwarzania przez Administratora Danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur ich przetwarzania, jak również są informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym.
 8. System informatyczny Administratora danych zabezpieczony jest programem antywirusowym, którego celem jest uniknięcie uzyskania nieuprawnionego dostępu do systemu informatycznego
 9. Pracownik jest zobowiązany zablokować system operacyjny (poprzez równoczesne wciśnięcie klawiszy Ctrl+Alt+Del), jeśli z jakiegokolwiek powodu pozostawia komputer bez nadzoru.
 10. Ani identyfikator ani hasło osoby, która utraciła upoważnienie do przetwarzania danych nie może być przydzielony innej osobie.
 11. Szczegółowe zasady przydzielania hasła i identyfikatora osobom upoważnionym określa Instrukcja Zarządzania Systemem Informatycznym.
 6. The employees have access to applications containing the personal data related to the performance of their employee responsibilities.
 7. The employees who process the personal data are obliged under non-disclosure agreements executed with the Controller to keep these data confidential. Before granting the access to process the personal data these persons are trained by the Controller on the applicable provisions on the processing of the personal data and the procedures as well as they are informed about the basic risks related to processing of the personal data in IT system.
 8. The Controller's IT system is protected by the antivirus software which purpose is to avoid non authorized access to the IT system.
 9. An employee shall lock OS (by simultaneous pressing Ctrl+Alt+Del) if leaving the portable computer unattended by whatever reason.
 10. Neither ID nor the password of a person who lost the authorization to process the personal data can be assigned to another person.
 11. The detailed rules on the password and the ID assignment to the authorized person are set forth in the System Security Instruction.

- | | |
|--|---|
| <p>12. Dane osobowe znajdujące się w zbiorze danych zabezpieczone są poprzez wykonanie kopii zapasowych na zasadach określonych w Instrukcji Zarządzania Systemem Informatycznym.</p> <p>13. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.</p> <p>14. Nośniki informacji zawierające dane osobowe znajdujące się w zbiorze danych przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych. Jeżeli nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.</p> <p>15. Nośniki informacji zawierające dane osobowe znajdujące się w zbiorze danych przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu. tych danych, w sposób uniemożliwiający ich odzyskanie.</p> <p>16. Nośniki informacji zawierające dane osobowe znajdujące się w zbiorze danych przeznaczone do naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Danych.</p> <p>17. System informatyczny Administratora Danych chroni się przed zagrożeniami pochodzącymi z sieci za pomocą środków umożliwiających kontrolę przepływu informacji pomiędzy systemem a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu.</p> <p>18. Wyznaczono Administratora Bezpieczeństwa</p> | <p>12. The personal data stored in the filing system are secured by performing the backup under the rules set forth in the System Security Instruction.</p> <p>13. The means of protection against malicious software as for example bugs, viruses, Trojans and rootkits are used.</p> <p>14. The media which contain the personal data stored in the filing system and which are intended to liquidation shall be firstly deprived of its record. If such a deprivation is not possible the media shall be damaged in a way which makes its reading no more possible.</p> <p>15. The media which contain the personal data stored in the filing system and which are intended for the delivery to the entity unauthorized to process the data shall be firstly deprived of its record in a way which makes its recovery no more possible.</p> <p>16. The media which contain the personal data stored in the filing system and which are intended to be repaired shall be firstly deprived of its record in a way which makes its recovery no more possible or it shall be repaired under the supervision of the person authorized by the Controller.</p> <p>17. The Controller's IT system is protected against the risks originating from the network by the use of means which permit to control the data transfer between the system and the public network and control of the actions initiated in the public network and in the system.</p> <p>18. The Personal Data Protection Official shall</p> |
|--|---|

- | | |
|--|--|
| <p>Informacji.</p> <p>19. Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, o której mowa w § 2 pkt. 3.</p> <p>20. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych. Ewidencja zawiera imię, nazwisko pracownika, datę nadania uprawnień, datę odebrania uprawnień oraz zakres dostępu.</p> <p>21. Administrator Danych na bieżąco monitoruje wdrożone zabezpieczenia systemu informatycznego.</p> | <p>be appointed.</p> <p>19. As it was defined in § 2 section 3 the System Security Instruction applied to the personal data processing system shall be established.</p> <p>20. The registry of the persons authorized to process the personal data is conducted. The registry contains the employee's name, surname, the date when the access was granted, the date when the access was withdrawn and the scope of the access.</p> <p>21. The Controller monitors regularly the means enforced to protect the IT system.</p> |
|--|--|