KLAUZULA INFORMACYJNA RODO

dla pracowników, współpracowników, użytkowników systemów informatycznych, klientów, kontrahentów i partnerów biznesowych Działu IT Chińsko-Polskiego Towarzystwa Okrętowego S.A. w Szanghaju Oddział w Gdyni

1. Administrator danych osobowych

Administratorem danych osobowych jest Chińsko-Polskie Towarzystwo Okrętowe S.A. w Szanghaju Oddział w Gdyni z siedzibą przy ul. Śląskiej 17, 81-319 Gdynia, NIP: 5860104523, REGON: 001372525.

2. Inspektor Ochrony Danych

Administrator wyznaczył Inspektora Ochrony Danych. Kontakt z Inspektorem możliwy jest pod adresem e-mail: cp-gdpr@chipolbrok.com.pl.

3. Cele i podstawy prawne przetwarzania danych osobowych

Dane osobowe są przetwarzane w szczególności w celu:

- administrowania systemami informatycznymi, siecią teleinformatyczną oraz infrastrukturą IT Administratora;
- zarządzania tożsamością użytkowników, tworzenia, modyfikowania i usuwania kont użytkowników oraz nadawania, zmiany i odbierania uprawnień dostępu do systemów informatycznych;
- zapewnienia poufności, integralności, dostępności i odporności systemów oraz usług przetwarzania danych osobowych;
- monitorowania działania systemów informatycznych, infrastruktury teleinformatycznej, logów systemowych oraz bezpieczeństwa środowiska IT;
- monitorowania służbowej poczty elektronicznej zgodnie z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi Administratora;
- wykonywania, przechowywania i odtwarzania kopii zapasowych systemów oraz danych;
- świadczenia wsparcia technicznego użytkownikom systemów informatycznych;
- zapewnienia cyberbezpieczeństwa oraz ochrony zasobów informacyjnych Administratora;
- ustalenia, dochodzenia lub obrony przed roszczeniami;
- wypełnienia obowiązków wynikających z przepisów prawa.

Podstawy prawne:
- art. 6 ust. 1 lit. b RODO – wykonanie umowy lub podjęcie działań przed zawarciem

umowy;
- art. 6 ust. 1 lit. c RODO – wypełnienie obowiązku prawnego ciążącego na administratorze, w szczególności obowiązków związanych z zapewnieniem bezpieczeństwa przetwarzania danych osobowych;
- art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes administratora, w szczególności zapewnienie bezpieczeństwa systemów informatycznych i infrastruktury teleinformatycznej, zarządzanie uprawnieniami użytkowników, zapewnienie ciągłości działania systemów, ochrona danych osobowych oraz ustalenie, dochodzenie lub obrona przed roszczeniami.

4. Kategorie danych osobowych

Przetwarzane dane obejmują w szczególności: imię i nazwisko, służbowy adres e-mail, numer telefonu, identyfikator użytkownika, identyfikatory systemowe i sieciowe, informacje dotyczące nadanych uprawnień, adresy IP, logi systemowe, informacje dotyczące urządzeń wykorzystywanych do uzyskania dostępu do systemów Administratora, dane zawarte w kopiach zapasowych oraz inne dane niezbędne do zapewnienia prawidłowego funkcjonowania systemów informatycznych.

5. Źródło danych

Dane osobowe pochodzą od osoby, której dotyczą, oraz z innych źródeł, w szczególności z Działu HR, z systemów informatycznych Administratora, z infrastruktury teleinformatycznej, z urządzeń wykorzystywanych do pracy, od innych jednostek organizacyjnych Administratora.

6. Odbiorcy danych

Odbiorcami danych mogą być w szczególności podmioty świadczące usługi serwisowe dotyczące sprzętu komputerowego oraz infrastruktury IT, dostawcy oprogramowania, producenci oprogramowania, dostawcy usług informatycznych i cyberbezpieczeństwa, podmioty świadczące usługi utrzymania systemów informatycznych, podmioty świadczące usługi wykonywania i przechowywania kopii zapasowych, organy administracji publicznej oraz inne podmioty uprawnione na podstawie przepisów prawa.

7. Przekazywanie danych poza EOG

Dane mogą być przekazywane do państw trzecich. W takich przypadkach zapewnia się odpowiedni poziom ich ochrony zgodnie z przepisami RODO, w szczególności poprzez stosowanie odpowiednich zabezpieczeń przewidzianych w rozdziale V RODO, w tym standardowych klauzul.

8. Okres przechowywania danych

Dane osobowe będą przechowywane przez okres niezbędny do realizacji celów przetwarzania, a następnie przez okres wynikający z przepisów prawa oraz zasad archiwizacji obowiązujących u Administratora. Kopie zapasowe poczty elektronicznej przechowywane są przez okres trzech (3) lat.

9. Prawa osób, których dane dotyczą

Przysługuje Pani/Panu prawo do:
- dostępu do treści swoich danych,
- ich sprostowania,
- usunięcia danych („prawo do bycia zapomnianym”),
- ograniczenia przetwarzania,
- wniesienia sprzeciwu wobec przetwarzania,
- przenoszenia danych,
- wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.

10. Zautomatyzowane podejmowanie decyzji

Dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

11. Systemy informatyczne

W przetwarzaniu danych osobowych wykorzystywane są w szczególności: Microsoft Active Directory, Microsoft Exchange/Outlook, e-Auditor, ODMS, Symfonia, systemy wykonywania kopii zapasowych oraz inne systemy wspierające zarządzanie infrastrukturą teleinformatyczną i bezpieczeństwem informacji.

12. Dane szczególnej kategorii

Dział IT nie przetwarza danych szczególnych kategorii we własnych celach. Dział IT administruje jednak systemami informatycznymi, w których dane szczególnych kategorii mogą być przetwarzane przez inne jednostki organizacyjne Administratora. Dostęp administratorów systemów do takich danych może wystąpić wyłącznie w zakresie niezbędnym do zapewnienia prawidłowego funkcjonowania systemów, bezpieczeństwa informacji, usuwania awarii, wykonywania kopii zapasowych oraz realizacji czynności serwisowych.

GDPR INFORMATION CLAUSE

for employees, contractors, users of IT systems, customers, contractors and business partners of the IT Department of Chińsko-Polskie Towarzystwo Okrętowe S.A. in Shanghai, Gdynia Branch

1. Controller of the personal data

The Controller of the personal data is Chińsko-Polskie Towarzystwo Okrętowe S.A. in Shanghai, Gdynia Branch, with its registered office at ul. Śląska 17, 81-319 Gdynia, Poland, Tax Identification Number (NIP): 5860104523, Business Statistical Number (REGON): 001372525.

2. Data Protection Officer

The Controller has appointed a Data Protection Officer. The Data Protection Officer can be contacted by e-mail at: cp-gdpr@chipolbrok.com.pl.

3. Purposes and legal basis for the processing of personal data

Personal data is processed in particular for the following purposes:

- administration of the Controller's IT systems, ICT network and IT infrastructure;
- identity and access management, including the creation, modification and deletion of user accounts, as well as granting, modifying and revoking access rights to IT systems;
- ensuring the confidentiality, integrity, availability and resilience of IT systems and personal data processing services;
- monitoring the operation of IT systems, ICT infrastructure, system logs and the security of the IT environment;
- monitoring corporate e-mail in accordance with applicable laws and the Controller's internal regulations;
- creating, maintaining and restoring systems and data backups;
- providing technical support to users of the Controller's IT systems;
- ensuring cyber security and protecting the Controller's information assets;
- establishing, exercising or defending legal claims;
- complying with legal obligations.

Legal basis:

- Article 6(1)(b) GDPR – performance of a contract or taking steps prior to entering into a contract;

- Article 6(1)(c) GDPR – compliance with a legal obligation to which the Controller is subject, in particular obligations relating to ensuring the security of personal data processing;
- Article 6(1)(f) GDPR – the legitimate interests pursued by the Controller, in particular ensuring the security of IT systems and ICT infrastructure, managing user access rights, ensuring business continuity, protecting personal data, and establishing, exercising or defending legal claims.

4. Categories of personal data

The personal data processed includes, in particular, first name and last name; business e-mail address; telephone number; user identifier; system and network identifiers; information relating to assigned user permissions; IP addresses; system logs; information relating to devices used to access the Controller's IT systems; data contained in backup copies and other data necessary to ensure the proper operation of the Controller's IT systems.

5. Source of personal data

Personal data is obtained from the data subject and from other sources, in particular from the HR Department, the Controller's IT systems, ICT infrastructure, devices used for work, and other organisational units of the Controller.

6. Recipients of personal data

Recipients of personal data may include, in particular, entities providing maintenance services for computer hardware and IT infrastructure, software vendors and software licensors, providers of IT and cybersecurity services, entities providing maintenance and support services for IT systems, entities providing backup and data storage services, as well as public authorities and other entities authorised under applicable law.

7. Transfers of personal data outside the EEA

Data may be transferred to third countries. Where such transfers occur. The Controller ensures an adequate level of data protection in accordance with the GDPR, in particular by implementing appropriate safeguards provided for in Chapter V of the GDPR, including the Standard Contractual Clauses approved by the European Commission.

8. Data retention period

Personal data will be retained for the period necessary to fulfil the purposes of processing and thereafter for the period required by applicable law and the Controller's document retention rules. Backup copies of corporate e-mail are retained for three (3) years.

9. Rights of data subjects

You have the right to:

- access your personal data;
- rectify your personal data;
- erase your personal data ("right to be forgotten");
- restrict the processing of your personal data;
- object to the processing of your personal data;
- data portability;
- lodge a complaint with supervisory authority (in Poland: The President of the Personal Data Protection Office).

10. Automated decision-making

Personal data is not subject to automated decision-making, including profiling.

11. IT systems

The processing of personal data involves, in particular, the following systems and tools: Microsoft Active Directory, Microsoft Exchange/Outlook, e-Auditor, ODMS, Symfonia, backup systems, and other systems supporting the management of ICT infrastructure and information security.

12. Special categories of personal data

The IT Department does not process special categories of personal data for its own purposes. However, the IT Department administers IT systems in which special categories of personal data may be processed by other organisational units of the Controller. Access to such data by system administrators may occur solely to the extent necessary to ensure the proper functioning of IT systems, information security, fault resolution, backup operations and the performance of maintenance activities.