elektrotim

POLITYKA OCHRONY DANYCH OSOBOWYCH

POLITYKA OCHRONY DANYCH OSOBOWYCH W ELEKTROTIM S.A.

§ 1.
Postanowienia ogólne.

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**" (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w **ELEKTROTIM S.A.** z siedzibą we Wrocławiu.

2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

3. Polityka zawiera:
   a. opis zasad ochrony danych obowiązujących w Spółce;
   b. odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

4. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Spółki, a w ramach Zarządu:
   a. Członek Zarządu, któremu powierzono nadzór nad obszarem ochrony danych osobowych;
   b. osoba wyznaczona przez Zarząd do zapewnienia zgodności z ochrona danych osobowych.

5. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
   a. osoba wyznaczona przez Zarząd;
   b. komórka audytu wewnętrznego.

6. Za stosowanie niniejszej Polityki odpowiedzialni są:
   a. Spółka;
   b. komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji;
   c. komórki organizacyjne przetwarzające dane osobowe w dużym rozmiarze;
   d. pozostałe komórki organizacyjne;
   e. wszyscy członkowie personelu Spółki.

7. Spółka zapewnia zgodność postępowania kontrahentów Spółki z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

elektrotim

POLITYKA OCHRONY DANYCH OSOBOWYCH

§ 2.
Definicje.

Użyte w niniejszej Polityce pojęcia oznaczają:

a. **Polityka** - niniejsza Polityka ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

b. **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

c. **Dane** oznaczają – o ile co innego nie wynika wyraźnie z kontekstu, dane osobowe, czyli wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

d. **Dane specjalne** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

e. **Dane wrażliwe** oznaczają dane specjalne oraz dane karne.

f. **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

g. **Podmiot przetwarzający** – organizacja lub osoba, której Spółka powierzyła przetwarzanie danych osobowych.

h. Eksport danych – przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

i. IOD lub Inspektor – Inspektor Ochrony Danych Osobowych .

j. RCP – Rejestr Czynności Przetwarzania Danych Osobowych.

k. RKCP – Rejestr Kategorii Czynności Przetwarzania Danych Osobowych.

l. Spółka – ELEKTROTIM S.A. z siedzibą we Wrocławiu.

§ 3.
Cel i zakres stosowania Polityki.

1. Celem Polityki jest określenie postępowania gwarantującego bezpieczeństwo przetwarzanych danych osobowych w Spółce, poprzez podejmowanie działań zapewniających ich poufność, integralność, dostępność i rozliczalność.

2. Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie dane osobowe przetwarzane w Spółce, zarówno w formie elektronicznej, jak i papierowej.
3. Obszar, w ramach którego przetwarzane są informacje, w tym dane osobowe, obejmuje budynki Spółki.
4. Obszar, o którym mowa w ust. 3, obejmuje również budynki i pomieszczenia podmiotów zewnętrznych, którym na podstawie zawartych umów powierzono przetwarzanie danych osobowych, w zakresie niezbędnym do wykonywania zadań Spółki i prowadzenia przez nią działalności gospodarczej.

§ 4.
Ogólne zasady ochrony danych osobowych.

1. Ochrona danych osobowych w Spółce oparta została na następujących filarach:
   a. Legalność – Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
   b. Bezpieczeństwo – Spółka zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
   c. Prawa Jednostki – Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
   d. Rozliczalność – Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
2. Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:
   a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   b. rzetelnie i uczciwie (rzetelność);
   c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
   d. w konkretnych celach i nie „na zapas" (minimalizacja);
   e. nie więcej niż potrzeba (adekwatność);
   f. z dbałością o prawidłowość danych (prawidłowość);nie dłużej niż potrzeba
   g. (czasowość);
   h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 5.
System ochrony danych osobowych.

System ochrony danych osobowych w Spółce składa się z następujących elementów:

a. **Inwentaryzacja danych.** Spółka dokonuje identyfikacji zasobów danych osobowych w Spółce, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
   - przypadków przetwarzania danych specjalnych i wrażliwych;
   - przypadków przetwarzania danych osób, których Spółka nie identyfikuje (dane niezidentyfikowane);
   - współadministrowania danymi.

b. **Rejestry.** Spółka opracowuje, prowadzi i utrzymuje:
   - Rejestr Czynności Przetwarzania Danych Osobowych,
   - Rejestr Kategorii Czynności Przetwarzania Danych Osobowych,

- Rejestr naruszeń,
- Rejestr upoważnień i poleceń,
- Rejestr udostępnień.

Prowadzone Rejestry są narzędziem rozliczania zgodności z ochroną danych w Spółce.

c. **Polityki / Procedury.** Spółka opracowuje, wdraża i weryfikuje stosowanie Polityk / (Procedur) mających na celu zapewnienie należytego poziomu ochrony danych osobowych, w tym:
   - Politykę czystego biurka;
   - Politykę czystego ekranu;
   - Politykę czystej drukarki;
   - Politykę czystego kosza;
   - Politykę czystej tablicy;
   - Politykę kluczy;
   - Politykę odpowiedzialności za zasoby.

d. **Podstawy prawne.** Spółka zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych.

e. **Obsługa praw jednostki.** Spółka spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane żądania.

f. **Obsługa żądań.** Spółka zapewnia, aby żądania osób, których dane dotyczą były realizowane w terminach i w sposób wymagany RODO oraz odpowiednio dokumentowane.

g. **Zawiadamianie o naruszeniach**. Spółka stosuje procedury, w oparciu o które powiadamia organ nadzorczy i w określonych sytuacjach Administratora oraz pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

h. **Minimalizacja.** Spółka przetwarza Dane wyłącznie w zakresie niezbędnym do realizacji celu, dla którego zostały one zebrane oraz wprowadza zasady reglamentacji i zarządzania dostępem do danych, a także zarządza okresem przechowywania Danych i weryfikacji dalszej ich przydatności.

i. **Bezpieczeństwo.** Spółka dąży do zapewnienia odpowiedniego poziomu bezpieczeństwa danych.

j. **Powierzenie przetwarzania danych osobowych.** Spółka korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by powierzenie przetwarzania danych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Z każdym podmiotem przetwarzającym Spółka zawiera umowy powierzenia przetwarzania danych osobowych, stosownie do art. 28 RODO.

k. **Eksport danych.** Spółka weryfikuje, czy przekazuje bądź nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewni zgodne z prawem warunków takiego przekazywania, jeśli miałoby ono miejsce.

l. **Przetwarzanie transgraniczne**. Spółka weryfikuje, kiedy zachodzą przypadki przetwarzania transgranicznego oraz w razie potrzeby ustali zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

§ 6.
Bezpieczeństwo danych osobowych.

1. Spółka wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Spółka uwzględnia przy tym stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania.
2. Przy ocenie, czy stopień bezpieczeństwa jest odpowiedni, Spółka uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. W celu zapewnienia integralności i poufności Danych Spółka zapewnia dostęp do Danych jedynie osobom upoważnionym i wyłącznie w zakresie, w jakim jest to niezbędne ze względu na wykonywane przez nie zadania.
4. Spółka przeprowadza analizę ryzyka związanego z przetwarzaniem Danych i monitoruje adekwatność stosowanych zabezpieczeń Danych do identyfikowanych zagrożeń. W razie konieczności Spółka wdraża dodatkowe środki służące zwiększeniu bezpieczeństwa Danych.
5. W przypadku gdy rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Spółka przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony Danych osobowych.

§ 7.
Rejestry.

1. Spółka dążąc do wywiązania się z zasady rozliczalności, na której opiera się system ochrony danych osobowych prowadzi następujące rejestry:
   a. Rejestr Czynności Przetwarzania Danych Osobowych (RCP), w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe w odniesieniu do których jest Administratorem;
   b. Rejestr Kategorii Czynności Przetwarzania Danych Osobowych (RKCP), w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe w odniesieniu do których jest Podmiotem przetwarzającym;

c. Rejestr naruszeń,
d. Rejestr upoważnień i poleceń,

2. RCP i RKCP są jednym z podstawowych narzędzi umożliwiających Spółce wykazania zgodności z zasadą rozliczalności większości obowiązków ochrony danych, a także stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
3. Wzór RCP stanowi **Załącznik nr 1** do Polityki, wzór RKCP stanowi **Załącznik nr 2** do Polityki. Wzory RCP i RKCP zawierają także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Spółka rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem okoliczności, iż pełniejsza treść RCP i RKCP ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.
4. Spółka prowadzi Rejestr Naruszeń, w którym odnotowuje wszelkie incydenty związane z ochroną danych osobowych, m.in. w celu monitorowania oraz poprawy stosowanych zabezpieczeń, w celu zapewnienia odpowiedniego poziomu ochrony danych osobowych, które przetwarza. Wzór Rejestru naruszeń stanowi załącznik do Instrukcji I.51 Incydenty (Formularz I.51 – F.4 Rejestr naruszeń danych osobowych).
5. Spółka prowadzi Rejestr upoważnień i poleceń, w którym odnotowuje komu, kiedy i w jakim zakresie zostało udzielone upoważnienie i polecenie przetwarzania danych, a także kiedy upoważnienie i polecenie zostało odwołane. Wzór Rejestru upoważnień i poleceń stanowi załącznik do Instrukcji I.26 Bezpieczeństwo osobowe (Formularz I.26 – F.9 Rejestr osób upoważnionych do przetwarzania).

§ 8.
Podstawy przetwarzania danych osobowych.

1. Spółka dokumentuje w Rejestrze czynności przetwarzania podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Wskazując ogólną podstawę prawną, o jakiej mowa w art. 6 ust. 1 RODO, Spółka dookreśla podstawę w sposób jasny, czytelny i zrozumiały (np. w przypadku, w którym podstawą przetwarzania jest zgoda, wskazuje na jej zakres, gdy podstawą jest przepis prawa – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń).
3. Spółka wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
4. Kierownik komórki organizacyjnej Spółki ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych (art. 6 ust. 1 RODO). Jeżeli podstawą jest uzasadniony interes Spółki (art. 6 ust. 1 lit. f RODO), kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Spółki.

§ 9.
Sposób obsługi praw jednostki i obowiązków informacyjnych.

1. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza tj. aby wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.
2. Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Spółki informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką w tym celu, itp.
3. Spółka dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
4. Spółka wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
5. W celu realizacji praw jednostki Spółka zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Spółkę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
6. Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

§ 10.
Obowiązki informacyjne.

1. Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Spółka informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby. Wzór klauzuli informacyjnej stanowi **Załącznik nr 3** do Polityki. Wzór klauzuli informacyjnej na potrzeby procesu rekrutacji stanowi **Załącznik nr 4** do Polityki. Wzór klauzuli informacyjnej dla Pracowników stanowi **Załącznik nr 5** do Polityki.
4. Spółka informuje osobę o przetwarzaniu jej danych przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej. Wzór klauzuli informacyjnej stanowi **Załącznik nr 3** do Polityki.
5. Spółka określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
6. Spółka informuje osobę o planowanej zmianie celu przetwarzania danych.
7. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.
8. Spółka informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
9. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
10. Spółka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

§ 11.
Realizacja żądań osób, których dane dotyczą.

1. Realizując prawa osób, których dane dotyczą, Spółka wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Spółka może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. Spółka informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. Spółka informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. Na żądanie osoby dotyczące dostępu do jej danych, Spółka informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Spółka nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
5. Na żądanie Spółka wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Spółka wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.
6. Spółka dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane dotyczą. Spółka ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.
7. Spółka uzupełnia i aktualizuje dane na żądanie osoby, której dane dotyczą. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Spółka nie musi przetwarzać danych, które są Spółce zbędne). Spółka może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Spółkę procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. Na żądanie osoby, Spółka usuwa dane, gdy:
    a. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
    b. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
    c. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
    d. dane były przetwarzane niezgodnie z prawem,
    e. konieczność usunięcia wynika z obowiązku prawnego,
9. Spółka określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad

ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

10. Jeżeli dane podlegające usunięciu zostały upublicznione przez Spółkę, Spółka podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.
11. W przypadku usunięcia danych Spółka informuje osobę o odbiorcach danych, na żądanie osoby, której dane dotyczą.
12. Spółka dokonuje ograniczenia przetwarzania danych na żądanie osoby, której dane dotyczą, gdy:
    a. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
    b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
    c. Spółka nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
    d. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
13. W trakcie ograniczenia przetwarzania Spółka przechowuje dane, natomiast nie przetwarza ich w inny sposób (np. nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
14. Spółka informuje osobę, której dane dotyczą przed uchyleniem ograniczenia przetwarzania.
15. W przypadku ograniczenia przetwarzania danych Spółka informuje, na żądanie osoby, której dane dotyczą, o odbiorcach danych.
16. Na żądanie osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki.
17. Jeżeli osoba, której dane dotyczą zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
18. Jeżeli Spółka prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych osoba, której dane dotyczą może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Spółka uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

§ 12.
Minimalizacja przetwarzanych danych osobowych.

1. Spółka dba o minimalizację przetwarzania danych pod kątem:
   a. adekwatności danych do celów (tj. ilości danych i zakresu przetwarzania),
   b. dostępu do danych,
   c. czasu przechowywania danych.
2. Spółka weryfikuje, pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO:
   a. zakres pozyskiwanych danych,
   b. zakres przetwarzania danych,
   c. ilość przetwarzanych danych.
3. Spółka stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
4. Spółka stosuje kontrolę dostępu fizycznego.
5. Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
6. Spółka dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje je.
7. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Spółki.
8. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych Spółki, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§ 13.
Dostęp podmiotów zewnętrznych.

1. Przetwarzanie danych osobowych zgromadzonych w Spółce może zostać powierzone podmiotowi zewnętrznemu. Spółka korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Przetwarzanie przez podmiot przetwarzający odbywa się, zgodnie ze wskazanymi art. 28 RODO, na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:
   a. przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora - co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada

na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje Spółkę o tym obowiązku prawnym,

b. o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
c. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
d. podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
e. przestrzega warunków korzystania z usług dalszego podmiotu przetwarzającego, zgodnie z postanowieniami zawartej umowy powierzenia;
f. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Spółce poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
g. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Spółce wywiązać się z obowiązków określonych w art. 32-36 RODO;
h. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Spółki usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
i. udostępnia Spółce wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez Spółkę przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

3. Umowa powierzenia przetwarzania pomiędzy Spółką a Podmiotem przetwarzającym powinna zostać zawarta w formie pisemnej. W wyjątkowych przypadkach, uzasadnionych w szczególności okolicznościami w jakich następuje powierzanie przetwarzania, Spółka – w drodze wyjątku – w formie elektronicznej. Wzór umowy powierzenia stanowi do Instrukcji I.51 Incydenty (Załącznik I.02 – Z.3 Umowa powierzenia danych osobowych).

§ 14.
Upoważnienia i polecenia przetwarzania danych osobowych.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienia, którym Spółka poleciła przetwarzanie danych w zakresie wskazanym w dokumencie upoważnienia i polecenia przetwarzania danych, którego wzór stanowi załącznik do Instrukcji I.26 Bezpieczeństwo osobowe (Formularz I.26 – F.7 Upoważnienie i polecenie do przetwarzania danych osobowych).

6. Nadanie i odwołanie upoważnień do przetwarzania danych osobowych odbywa się na wniosek kierownika komórki organizacyjnej, który przekazywany jest do Spółki. Na podstawie zatwierdzonego przez Spółkę wniosku, osoba wyznaczona przez Spółkę sporządza upoważnienie do przetwarzania danych osobowych / odwołanie upoważnienia i przekazuje do zatwierdzenia przez Spółkę. Wzór wniosku o nadanie, odwołanie upoważnienia i polecenia przetwarzania danych osobowych stanowi

załącznik do Instrukcji I.26 Bezpieczeństwo osobowe (Formularz I.26 – F.6 Wniosek o nadanie_odwołanie upoważnienia).

2. Uprawnienia do przetwarzania danych osobowych wskazane w upoważnieniu i poleceniu przetwarzania wynikają z zakresu zadań służbowych pracownika.
7. Upoważnienie i polecenie przetwarzania danych może być odwołane w każdym czasie. Upoważnienia nadawane są na czas trwania stosunku pracy lub na czas określony i nie wymagają odrębnego odwołania. Upoważnienie i odwołanie upoważnienia sporządzane jest w dwóch egzemplarzach, po jednym dla każdej ze Stron. Wzór odwołania upoważnienia i polecenia przetwarzania danych osobowych stanowi załącznik do Instrukcji I.26 Bezpieczeństwo osobowe (Formularz I.26 – F.8 Odwołanie upoważnienia do przetwarzania danych osobowych).
8. Osoba wyznaczona przez Spółkę prowadzi elektroniczną ewidencję nadanych i odwołanych upoważnień oraz przechowuje dokumenty w wersji papierowej. Wzór Rejestru upoważnień i poleceń stanowi załącznik do Instrukcji I.26 Bezpieczeństwo osobowe (Formularz I.26 – F.9 Rejestr osób upoważnionych do przetwarzania).
9. Nadanie upoważnienia i udzielenie polecenia przetwarzania danych osobowych poprzedzone jest szkoleniem Pracownika Spółki z zakresu ochrony danych osobowych.

§ 15.
Techniczne i organizacyjne środki ochrony danych osobowych.

1. Spółka jest obowiązany do zastosowania środków organizacyjnych i technicznych, zapewniających bezpieczeństwo i ochronę przetwarzanych danych osobowych, bez względu na formę ich przetwarzania.
2. W Spółce stosuje się następujące systemy zabezpieczeń przed nieuprawnionym dostępem do danych osobowych:
    a. zabezpieczenia pomieszczeń, składających się na obszar przetwarzania danych osobowych: w
        - przypadku opuszczenia pomieszczenia, w którym przetwarza się dane osobowe, przez ostatnią osobę, pomieszczenie zamykane jest na klucz, także w godzinach pracy,
        - po godzinach pracy klucze do pomieszczeń, w których przetwarzane są dane osobowe, przechowywane są w dyspozytorze przy recepcji,
        - dane osobowe przechowywane w formie papierowej lub elektronicznej na nośnikach po zakończeniu pracy przechowywane są w zamykanych szafach biurowych,
        - nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są niezwłocznie w niszczarkach lub umieszczane w specjalnych pojemnikach,
        - budynki Spółki są nadzorowane przez pracowników ochrony poza zwykłymi godzinami pracy spółki (tj. w godzinach 15:00 – 7:00) lub w uzasadnionych bieżącymi potrzebami Spółki – całodobowo oraz wyposażone w system alarmowy przeciwwłamaniowy i monitoring zewnętrzny,
        - uzyskanie dostępu do pomieszczeń znajdujących się w siedzibie Spółki możliwe jest jedynie za pomocą indywidualnej identyfikacyjnej karty zbliżeniowej,

- dostęp do siedziby Spółki kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych;

b. zabezpieczenia zbiorów danych osobowych w formie elektronicznej przed nieautoryzowanym dostępem:
   - identyfikacja użytkownika w systemie informatycznym wymaga zastosowania uwierzytelnienia,
   - niepowtarzalne indywidualne identyfikatory dla użytkowników systemu informatycznego,
   - udostępnianie użytkownikowi programów i baz danych, zawierających dane osobowe następuje na podstawie upoważnienia do przetwarzania danych osobowych, wydanego przez Spółkę,
   - podłączenie urządzenia końcowego do sieci komputerowej Spółki dokonywane jest przez Administratora Systemu Informatycznego lubi innej osoby do tego wyznaczonej;
   - odseparowanie wewnętrznej sieci komputerowej Spółki od sieci publicznej za pomocą urządzeń typu Firewall,
   - wyposażenie wszystkich stanowisk komputerowych w indywidualną ochronę antywirusową,
   - zabezpieczenie hasłami kont na komputerach oraz używanie kont z ograniczonymi uprawnieniami do ciągłej pracy,
   - automatyczne wygaszanie ekranu i blokowanie nieużywanego komputera po upływie określonego czasu,
   - wymuszanie okresowej zmiany hasła użytkownika,
   - ustawienie monitorów stanowisk komputerowych używanych do przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym,
   - udostępnianie kluczy i kart dostępu do serwerowni wyłącznie osobom do tego upoważnionym;

c. zabezpieczenia danych osobowych przed utratą w wyniku awarii:
   - zastosowanie zasilaczy zapasowych w celu ochrony serwerów przed skutkami zaniku zasilania,
   - cykliczne wykonywanie kopii zapasowych zgromadzonych danych, z których w przypadku awarii, odtwarzane są dane i system operacyjny,
   - zastosowanie klimatyzatorów w celu zapewnienia właściwej temperatury i wilgotności powietrza w serwerowniach,
   - rozmieszczenie gaśnic w serwerowniach;

d. stały nadzór nad systemem stosowanych zabezpieczeń:
   - pracownicy Spółki są obowiązani do zwracania uwagi na prawidłowość pracy systemów informatycznych, przestrzegania wewnętrznych procedur bezpieczeństwa oraz informowania przełożonych i Spółki o zauważonych lub potencjalnych nieprawidłowościach,
   - przetwarzanie danych osobowych dopuszczalne jest wyłącznie na zarejestrowanych: stacjach roboczych, komputerach przenośnych, nośnikach.

3. Uszkodzone lub wycofywane elektroniczne nośniki zawierające dane osobowe podlegają fizycznemu zniszczeniu. Każdorazowo sporządzany jest protokół zniszczenia.

4. Komputery podlegające naprawie przekazywane są do punktów serwisowych po wymontowaniu dysków twardych. Każdorazowo sporządzany jest protokół naprawy.

§ 16.
Polityka kluczy.

1. W Spółce obowiązuje ograniczony dostęp do pomieszczeń znajdujących się w siedzibie Spółki. Dostęp poszczególnych osób do pomieszczeń wewnętrznych jest uzasadniony potrzebami funkcjonowania Spółki. Szczegółowe zasady dotyczące bezpieczeństwa fizycznego i środowiskowego reguluje instrukcja I-46 „Bezpieczeństwo fizyczne i środowiskowe".
2. Spółka sprawuje nadzór nad kluczami do pomieszczeń, zgodnie z następującymi regułami:
    a. Możliwość pobierania kluczy do pomieszczeń Spółki z depozytora znajdującego się przy recepcji Spółki, mają jedynie osoby upoważnione do tego celu przez przełożonego.
    b. W godzinach pracy klucze do pomieszczeń pozostają pod nadzorem pracowników, którzy ponoszą za nie odpowiedzialność.
    c. Klucze do pomieszczeń szczególnie chronionych (np. serwerownia) mogą zostać pobrane jedynie przez upoważnioną do tego osobę. Dostęp osób trzecich do pomieszczeń szczególnie chronionych odbywa się pod nadzorem osób do tego upoważnionych.
    d. Klucze zapasowe przechowywane są przez Dział Infrastruktury. Wydawanie zapasowych kluczy może mieć miejsce wyłącznie w sytuacjach awaryjnych. Klucze zapasowe należy niezwłocznie po wykorzystaniu zwrócić.

§ 17.
Polityka czystego biurka.

1. Polityka czystego biurka obowiązuje wszystkich pracowników zatrudnionych w Spółce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
4. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
5. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej szafy.
6. Po zakończonej pracy pracownik zobowiązany jest odłożyć laptopa do zamykanej na szafy.
7. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
8. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

§ 18.
Polityka czystego ekranu.

1. Polityka czystego ekranu obowiązuje wszystkich pracowników zatrudnionych w Spółce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Każdy komputer wykorzystywany w celu świadczenia pracy na rzecz spółki, na którym są lub mogą znajdować się dane osobowe posiada szyfrowany dysk, którego uruchomienie uzależnione jest od podania hasła.
4. Każdy komputer wykorzystywany w celu świadczenia pracy na rzecz spółki, na którym są lub mogą znajdować się dane osobowe posiada jest zabezpieczony hasłem. Szczegółowe zasady tworzenia haseł dostępu zostały opisane w Załączniku 3 do Instrukcji I-50 (I-50 Z-3).
5. W przypadku każdorazowego opuszczenia miejsca pracy, pracownik korzystający z komputera powinien go zablokować w celu zabezpieczenia przed nieupoważnionym dostępem do danych na nim przetwarzanych poprzez włączenie wygaszacza ekranu lub – w przypadku dłuższej nieobecności, wylogować się z systemu.

§ 19.
Polityka czystego druku.

1. Polityka czystego druku obowiązuje wszystkich pracowników zatrudnionych w Spółce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Informacje drukowane powinny być zabierane z drukarek niezwłocznie po ich wydrukowaniu.
4. W przypadku nieudanej próby drukowania, pracownik powinien skontaktować się z osobą odpowiedzialną za poprawne funkcjonowanie urządzenia.
5. Pracownik jest zobowiązany samodzielnie lub – w razie potrzeby, z pomocą bądź według instrukcji pracownika odpowiedzialnego za funkcjonowanie urządzenia usunąć pliki z pamięci drukarki.
6. Niezwłocznie po wydrukowaniu pliku pracownik zobowiązany jest do wylogowania się z systemu drukującego Dokumaster.

§ 20.
Polityka czystego kosza.

1. Polityka czystego kosza obowiązuje wszystkich pracowników zatrudnionych w Spółce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Dokumenty papierowe z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych powinny być niszczone w sposób uniemożliwiający odczytanie z nich treści w szczególności danych osobowych.
4. Dokumenty powinny być niszczone w niszczarce doraźnie lub umieszczane w specjalnie przeznaczonych do tego pojemnikach.

§ 21.
Polityka czystej tablicy.

1. Polityka czystej tablicy obowiązuje wszystkich pracowników zatrudnionych w Spółce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Po zakończeniu zajęć, spotkań, dyskusji itp. z sali, w której odbywało się spotkanie należy uprzątnąć wszystkie materiały oraz oczyścić tablice.

§ 22.
Polityka odpowiedzialności za zasoby.

1. Polityka odpowiedzialności za zasoby obowiązuje wszystkich pracowników zatrudnionych w Spółce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Każdy pracownik odpowiada za udostępnione mu do realizacji celów służbowych zasoby Spółki, takie jak w szczególności: komputery, oprogramowanie, systemy i konta itp.).
4. Wykorzystanie zasobów Spółki do celów prywatnych możliwe jest jedynie w ograniczonym zakresie, po uzyskaniu zgody bezpośredniego przełożonego.
5. Zabronione jest instalowanie nielegalnego oprogramowania.

§ 23.
Inspektor ochrony danych osobowych.

1. Spółka, po przeprowadzeniu analizy art. 37-39 RODO, uznając, że nie podlega ona obowiązkowi powołania Inspektora Danych Osobowych, nie powołuje Inspektora.
2. Spółka może powołać wyznaczoną osobę do pełnienia funkcji kontrolera procesów przetwarzania danych osobowych, celem zapewnienia wysokiego standardu ochrony przetwarzanych przez nią danych osobowych. W przypadku wyznaczeniu takiej osoby Pracownicy Spółki zostaną niezwłocznie o tym poinformowani.
3. W przypadku powołania w spółce osoby mającej pełnić funkcję kontrolera procesów przetwarzania danych osobowych, zostanie przyjęty regulamin funkcjonowania kontrolera, w którym zostaną szczegółowo określone jego zadania i status.
4. W przypadku powołania w spółce osoby mającej pełnić funkcję kontrolera procesów przetwarzania danych osobowych Spółka może – w razie potrzeby – powołać również zespół wspierający kontrolera przy wykonywaniu powierzonych mu czynności.
5. Jeżeli w spółce nie zostanie powołany kontroler procesów przetwarzania danych osobowych, nad zgodnością dokumentacji i przestrzeganiem zasad przetwarzania danych osobowych czuwa inna wyznaczona osoba, której dane kontaktowe zostaną podane wszystkim Pracownikom Spółki.

§ 24.
Naruszenie zasad ochrony danych osobowych.

1. W przypadku naruszenia w Spółce ochrony danych osobowych, Prezes Spółki lub wyznaczona przez niego osoba bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie naruszenia w Spółce ochrony danych osobowych musi co najmniej:
   a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d. opisywać środki zastosowane lub proponowane przez DPS w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

   Wzór zgłoszenia naruszenia organowi nadzorczemu stanowi załącznik do Instrukcji I.51 Incydenty (Formularz I.51 – F.1 Zgłoszenie naruszenia ochrony danych osobowych do PUODO). Wzór zawiadomienia Administratora o naruszeniu zasad ochrony danych osobowych, tj. w sytuacji, w której Spółka jest podmiotem przetwarzającym dane, nie zaś ich Administratorem stanowi załącznik do Instrukcji I.51 Incydenty (Formularz I.51 – F.2 Zgłoszenie naruszenia danych osobowych

Administratorowi). Wzór zawiadomienia osoby, której dane dotyczą o wystąpieniu naruszenia stanowi załącznik do Instrukcji I.51 Incydenty (Formularz I.51 – F.3 Zawiadomienie osoby o naruszeniu danych osobowych). Raport zgłoszenia naruszenia stanowi **Załącznik nr 6** do niniejszej Polityki.

3. Spółka dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych w Spółce, jego skutki oraz podjęte działania zaradcze. Wzór Rejestru naruszeń stanowi załącznik do Instrukcji I.51 Incydenty (Formularz I.51 – F.4 Rejestr naruszeń danych osobowych).
4. Postępowanie w przypadku wystąpienia incydentu, tj. sytuacji naruszającej lub stwarzającej ryzyko naruszenia bezpieczeństwa danych osobowych, szczegółowo określają regulacje wewnętrzne Spółki, tj. Instrukcja I.51 – Incydenty.

§ 25.
Ochrona danych osobowych podczas pracy zdalnej.

1. Pracownik wykonujący pracę zdalnie, uzyskuje dostęp do danych osobowych, których przetwarzanie jest niezbędne do wykonywania obowiązków pracowniczych. Nie jest dopuszczalne wykorzystywanie danych osobowych przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków służbowych.
2. Pracownik wykonujący pracę zdalnie utrzymuje w tajemnicy otrzymane od pracodawcy dane dostępowe, w tym loginy i hasła oraz zabezpiecza je przed dostępem osób nieuprawnionych, w tym domowników.
3. Komunikacja służbowa przy wykonywaniu pracy zdalnie odbywa się w sposób zapewniający bezpieczeństwo informacji i danych osobowych, wyłącznie poprzez udostępnione przez pracodawcę narzędzia i połączenia, zgodnie z Regulaminem pracy zdalnej.
4. Pracownik wykonujący pracę zdalnie odpowiada za bezpieczne przechowywanie danych osobowych, sprzętu i nośników służących do ich przetwarzania. Nośniki oraz dokumentacja zawierająca dane osobowe nie powinna być pozostawiana bez nadzoru. Po zakończeniu pracy nośniki i dokumentacja powinny być schowane w miejscu zabezpieczonym przed osobami nieuprawnionymi.
5. Pracownik wykonujący pracę zdalnie zgłasza incydenty ochrony danych podczas pracy zdalnej oraz ich podejrzenia osobom odpowiedzialnym u Pracodawcy za ochronę danych osobowych.
6. W przypadku zauważania nieprawidłowości w funkcjonowaniu systemów informatycznych pracownik wykonujący pracę zdalnie podejmuje możliwe działania zabezpieczające jednocześnie z powiadomieniem Działu Informatyki.
7. Pracownik wykonujący pracę zdalnie odpowiada za bezpieczeństwo powierzonego mu sprzętu, nośników i dokumentacji podczas ich transportu. Przewożenie dokumentacji zawierającej dane osobowe powinno odbywać się w sposób zabezpieczający ją przed dostępem osób nieuprawnionych.
8. Pracownik wykonujący pracę zdalnie zobowiązany jest do dbałości o bezpieczeństwo danych osobowych przetwarzanych w ramach wykonywania obowiązków służbowych. W tym celu, podczas codziennej pracy pracownik wykonujący pracę zdalnie:

   a) ogranicza do niezbędnego minimum drukowanie plików zawierających dane osobowe i do sytuacji, gdy jest to konieczne;

b) niszczy robocze wydruki zawierające dane osobowe po ustaniu ich przydatności dla bieżącej pracy; nie można wyrzucać dokumentów zawierających dane osobowe do kosza, zniszczenie musi mieć charakter nieodwracalny, np. przy użyciu niszczarki lub nożyczek;
c) cyklicznie usuwa niepotrzebne pliki zawierające dane osobowe, pobrane w celu pracy z nimi;
d) przechowuje dokumentację zawierającą dane osobowe w sposób bezpieczny, w miejscu niedostępnym dla osób postronnych;
e) wylogowuje się z systemów informatycznych zarówno w przerwie od pracy, jak i po jej zakończeniu pracy;
f) zabezpiecza ekran przed dostępem innych osób, w tym domowników, poprzez stosowanie wygaszaczy ekranów lub każdorazowe wylogowanie się przed odejściem od ekranu;
g) nie korzysta i nie uruchamia programów i aplikacji pochodzących od nieznanych nadawców;
h) nie udostępnia domownikom komputerów przenośnych przeznaczonych do pracy, jeżeli komputer stanowi własność pracownika, praca odbywa się wyłącznie na wydzielonych kontach systemowych.

§ 26.
Postanowienia końcowe.

1. Do spraw nieuregulowanych w Polityce, w zakresie ochrony danych osobowych stosuje się przepisy RODO, ustawy o ochronie danych osobowych oraz innych regulacji, w tym regulacji wewnętrznych.
2. Wszystkie rejestry, ewidencje, wykazy, o których mowa w Polityce objęte są nakazem zachowania w tajemnicy.

Załączniki:

1. Wzór Rejestru Czynności Przetwarzania Danych.
2. Wzór Rejestru Kategorii Czynności Przetwarzania Danych Osobowych.
3. Wzór klauzuli informacyjnej.
4. Wzór klauzuli informacyjnej na potrzeby procesu rekrutacji.
5. Wzór klauzuli informacyjnej dla Pracowników.
6. Raport zgłoszenia naruszenia.

PREZES ZARZĄDU
ELEKTROTIM S.A.
/-/
Artur Więznowski

Metryczka dokumentu:

Poprzednie wydanie z dnia: 24.02.2023r.		
Opracował: Małgorzata Grygorcewicz Kierownik Działu Prawnego, Radca prawny Data: 17.04.2023r.		Zatwierdził: Artur Więznowski Prezes Zarządu, Dyrektor Generalny Data: 21.04.2023r.
Status dokumentu: nadzorowany	DOKUMENT DO UŻYTKU SŁUŻBOWEGO	Liczba załączników: 6