ARBONIA

Instrukcja dotycząca postępowania z danymi (Instrukcja dot. ochrony danych osobowych)

16 czerwca 2020

ARBONIA

SPIS TREŚCI

1 CEL I PRZEZNACZENIE 3
2 OKREŚLENIA POJĘĆ I DEFINICJE 4
3 ZAKRES 6
3.1 Zakres organizacyjny 6
3.2 Ustawy, rozporządzenia, standardy i instrukcje 6
4 PODSTAWY PRAWNE 7
5 ROLE I ZAKRESY OBOWIĄZKÓW 7
6 PODSTAWY OCHRONY DANYCH OSOBOWYCH DLA PRZETWARZANIA DANYCH OSOBOWYCH 10
6.1 Uczciwość, zgodność z prawem i transparentność 11
6.2 Cel wykorzystywania 12
6.3 Minimalizacja danych 12
6.4 Prawidłowe i aktualne 12
6.5 Ograniczony czas przechowywania 13
6.6 Poufność i bezpieczeństwo danych 13
7 DALSZE OBOWIĄZKI WYNIKAJĄCE Z RODO LUB INNYCH PODOBNYCH ROZPORZĄDZEŃ DOT. OCHRONY DANYCH OSOBOWYCH 13
7.1 Podstawa – obowiązek rozliczalności 13
7.2 Reguły dla podmiotów przetwarzających zlecenie (przede wszystkim partnerów w zakresie usług) 14
7.2.1 Udostępnianie danych osobowych podmiotowi przetwarzającemu zlecenie (wychodzące) 15
7.2.2 Odbiór danych osobowych jako podmiot przetwarzający zlecenie (przychodzące) 15
7.3 Przekazywanie danych osobowych do innych państw 15
7.4 Postępowanie z zapytaniami o informacje osób, których dane dotyczą. 16
7.5 Przeprowadzanie szacowania skutków dla ochrony danych osobowych 18
8 BEZPIECZEŃSTWO DANYCH OSOBOWYCH 19
9 ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM DANYCH 21
10 SKUTKI NIEPRZESTRZEGANIA 22
11 ODCHYLENIA 22
12 INFORMACJE 22
13 WEJŚCIE W ŻYCIE 22

ARBONIA

1 CEL I PRZEZNACZENIE

W celu spełnienia zobowiązań ustawowych i umownych niezbędne jest gromadzenie i przetwarzanie danych osobowych. Należy przy tym bezwzględnie przestrzegać obowiązujących w danym kraju przepisów dotyczących ochrony danych osobowych. Niniejsza instrukcja objaśnia w jaki sposób Arbonia AG i jej spółki koncernu (dalej nazywane łącznie „Arbonia" lub, gdy chodzi o jedną spółkę koncernu, „spółka koncernu") postępują z danymi osobowymi. Podane postanowienia stanowią standard minimalny. Jeśli lokalnie obowiązujące prawo zawiera bardziej wymagające przepisy ochrony danych, należy ich przestrzegać. Należy również przestrzegać wszelkich lokalnych przepisów związanych z realizacją niniejszej instrukcji.

Celem niniejszej instrukcji dotyczącej postępowania z danymi („Instrukcja dot. ochrony danych osobowych") jest określenie, realizacja, utrzymanie i stałe ulepszanie przestrzegania ochrony danych osobowych, zgodnie z wymaganiami rozporządzenia Unii Europejskiej o ochronie danych osobowych 2016/679 (**RODO**) oraz wszystkimi innymi obowiązującymi lokalnie przepisami ochrony danych osobowych (wraz z obowiązującymi **ustawami o ochronie danych osobowych**) przez firmę Arbonia.

Nieprzestrzeganie obowiązujących ustaw o ochronie danych osobowych wystawia firmę Arbonia na ryzyko szkód dla reputacji oraz poważne kary finansowe (np. do 4% rocznego obrotu zgodnie z RODO). Ponadto może wystawiać naszych klientów i pracowników na określone ryzyka związane z danymi osobowymi, np. kradzież tożsamości lub straty finansowe. Przestrzeganie obowiązujących ustaw o ochronie danych osobowych pomaga nam podtrzymywać zaufanie opinii publicznej wobec firmy Arbonia i wspiera pomyślną działalność firmy.

Celem niniejszej Instrukcji dot. ochrony danych osobowych jest określenie ram dla takiego przestrzegania wymogów ochrony danych osobowych wewnątrz koncernu Arbonia. W szczególności ma ona na celu realizację podstawowych zasad przetwarzania danych osobowych (**podstawy ochrony danych osobowych**) wymienionych w rozdziale 6 i obowiązujących dla spółek koncernu Arbonia, kiedy jako podmiot odpowiedzialny za przetwarzanie danych osobowych działają one w ramach RODO; ponadto reguluje on konieczność odpowiednich środków technicznych i organizacyjnych oraz zgłaszania przypadków naruszenia ochrony danych osobowych jako standardu minimalnego dla wszystkich przedsiębiorstw Arbonia; instrukcja obowiązuje dla wszystkich pracowników Arbonia oraz członków rady nadzorczej Arbonia AG.

Ponadto przygotowuje ona ramy dla dalszych wymagań, które obowiązują podmiot odpowiedzialny za przetwarzanie danych osobowych oraz podmiot przetwarzający zlecenie w ramach RODO (lub innych obowiązujących przepisów ochrony danych osobowych), jak to opisano w rozdziale 7.

2 OKREŚLENIA POJĘĆ I DEFINICJE

Dla celów niniejszej instrukcji dot. ochrony danych osobowych obowiązują następujące określenia pojęć i definicje:

Dane zanonimizowane oznaczają, że nie da się powiązać ich z tożsamością konkretnej osoby lub jest to możliwe tylko poprzez niewspółmierny nakład czasu, kosztów i pracy.

Obowiązujące ustawy o ochronie danych osobowych oznaczają rozporządzenie Unii Europejskiej o ochronie danych osobowych 2016/679 (**RODO**) lub wszystkie inne obowiązujące krajowe przepisy ochrony danych osobowych, obejmujące zbliżone przepisy.

Właściciel procesu biznesowego to osoba fizyczna odpowiedzialna w rozumieniu niniejszej instrukcji dot. ochrony danych osobowych i odpowiadająca za przetwarzanie danych osobowych oraz powiązane zastosowania IT.

Wyrażenie zgody oznacza wyrażenie zgody przez osobę, której dane dotyczą, czyli każdą udzieloną dobrowolnie, świadomie i jednoznacznie zgodę w formie deklaracji lub innej jednoznacznej formie, poprzez którą osoba, której dane dotyczą daje do zrozumienia, że zgadza się na przetwarzanie dotyczących jej danych osobowych.

Podmiot odpowiedzialny za przetwarzanie danych osobowych to osoba fizyczna lub prawna, urząd, agencja, lub inny podmiot, który samodzielnie lub we współpracy z innymi określa cele i środki przetwarzania danych osobowych.

Incydenty związane z danymi osobowymi oznaczają zdarzenia, w których istnieje podejrzenie, że dane osobowe zostały zarejestrowane, zebrane, zmienione, skopiowane, przekazane lub użyte w sposób niezgodny z prawem. Może to odnosić się również do działań osób trzecich lub pracowników.

Osoba, której dane dotyczą to zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można zidentyfikować bezpośrednio lub pośrednio, w szczególności poprzez przypisanie cechy identyfikacyjne, takiej jak imię i nazwisko, numer identyfikacyjny, dane lokalizacji, identyfikatory online lub jedną bądź więcej cech szczególnych wyrażonych w fizycznej, fizjologicznej, genetycznej, psychologicznej, kulturowej lub społecznej tożsamości danej osoby.

Podmiot przetwarzający zlecenie to osoba naturalna lub prawna, urząd, instytucja lub inny podmiot, przetwarzające dane osobowe na zlecenie podmiotu odpowiedzialnego za przetwarzanie danych osobowych.

Spis czynności przetwarzania oznacza listę wszystkich czynności przetwarzania danych odbywających się w zakresie odpowiedzialności podmiotu odpowiedzialnego za przetwarzanie danych osobowych. Spis ten zawiera wszystkie następujące dane: (i) nazwę

i dane kontaktowe podmiotu odpowiedzialnego za przetwarzanie danych osobowych oraz, jeśli dotyczy, podmiotów współodpowiedzialnych; przedstawiciela podmiotu odpowiedzialnego za przetwarzanie danych osobowych i lokalnego koordynatora ds. ochrony danych osobowych; (ii) cele przetwarzania; (iii) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych; (iv) kategorie odbiorców, którym udostępniono lub udostępnia się dane osobowe, łącznie z odbiorcami w krajach trzecich; (v) jeśli dotyczy, przekazywanie danych osobowych do krajów trzecich, łącznie z podaniem kraju trzeciego i udokumentowaniem występujących gwarancji bezpieczeństwa; (vi) przewidywany czas usunięcia różnych kategorii danych osobowych; (vii) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Pełnomocnik ds. ochrony danych osobowych lub koordynator ds. ochrony danych osobowych, inaczej **KDO**, oznacza osobę opisaną w rozdziale 5.

Dane osobowe oznaczają wszystkie informacje (łącznie ze szczególnymi kategoriami danych osobowych) na temat zidentyfikowanej lub identyfikowalnej osoby, której dane dotyczą; są to dane takie jak imię i nazwisko, data urodzenia, adres e-mail, wyznawana religia, dane lokalizacyjne, dane online (adresy IP, dane lokalizacyjne, itd.), numery identyfikacyjne (nr ubezpieczenia społecznego, nr dowodu osobistego itd.), cechy fizyczne (płeć, kolor skóry, włosów lub oczu, itd.), dane klienta itd.), które podlegają obowiązującemu rozporządzeniu dotyczącemu ochrony danych osobowych.

Przetwarzanie lub **przetwarzać** oznacza każdy proces lub szereg procesów związanych z danymi osobowymi, wykonywanych z pomocą procedur zautomatyzowanych lub bez; są to pozyskiwanie, rejestracja, organizacja, porządkowanie, zapisywanie, dostosowanie lub zmiana, odczyt, przeszukiwanie, użycie, publikacja poprzez przekazywanie, rozpowszechnianie lub każdą inną formę udostępniania; porównywanie lub powiązanie, ograniczanie, usuwanie lub niszczenie danych osobowych.

Pseudonimizacja oznacza przetwarzanie danych osobowych w sposób, w którym danych osobowych lub włączenia dodatkowych informacji nie można już przypisać do konkretnej osoby, której dane dotyczą, jeżeli te informacje dodatkowe są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym, które gwarantują, że danych osobowych nie da się przypisać zidentyfikowanej ani identyfikowalnej osoby fizycznej.

Szczególne kategorie danych osobowych oznaczają dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, karalności, członkostwie w związkach zawodowych zdrowiu lub orientacji seksualnej osoby, której dane dotyczą, a także dane genetyczne i biometryczne służące celowi jednoznacznej identyfikacji osoby fizycznej.

Kraje trzecie to wszystkie kraje nienależące do Unii Europejskiej ani Europejskiego Obszaru Gospodarczego lub kraje z konkretnym poziomem ochrony danych, który został uznany

przez Komisję Europejską jako odpowiedni (patrz lista krajów o odpowiednim poziomie ochrony danych osobowych:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Strona trzecia to każda strona inna niż osoba, której dane dotyczą, podmiot odpowiedzialny za przetwarzanie danych osobowych lub podmiot przetwarzający zlecenie (w tym partnerzy biznesowi, podwykonawcy, biura kredytowe i inne) oraz każda strona działająca pod bezpośrednią zwierzchnością podmiotu odpowiedzialnego za przetwarzanie danych osobowych lub podmiotu przetwarzającego zlecenie, której powierzono przetwarzanie danych osobowych. Przy przetwarzaniu danych osobowych za zezwoleniem podmiot przetwarzający zlecenie nie jest stroną trzecią w rozumieniu ustawy o ochronie danych osobowych, ponieważ prawnie jest zaliczany do podmiotów odpowiedzialnych za przetwarzanie danych osobowych.

3 ZAKRES

3.1 Zakres organizacyjny

Niniejsza Instrukcja dot. ochrony danych osobowych obowiązuje dla wszystkich spółek koncernu Arbonia, wszystkich pracowników Arbonia i wszystkich członków rady nadzorczej Arbonia AG. Są one prawnie wiążące dla każdej ze spółek koncernu.

3.2 Ustawy, rozporządzenia, standardy i instrukcje

Niniejsza Instrukcja dot. ochrony danych osobowych obejmuje wymagania RODO i międzynarodowe uznane podstawy ochrony danych osobowych, nie zastępując przy tym istniejących przepisów krajowych. Uzupełnia ona obowiązujące krajowe przepisy ustawowe ochrony danych. W przypadku konfliktów lub wyższych wymagań obowiązujące prawo krajowe ma priorytet nad niniejszą Instrukcją dot. ochrony danych osobowych. Należy przestrzegać treści niniejszej Instrukcji dot. ochrony danych osobowych również, gdy nie występuje odpowiednia legislacja krajowa.

Jeśli niniejsza Instrukcja dot. ochrony danych osobowych jest sprzeczna z postanowieniami obowiązującymi w danym kraju, można przyjąć lokalną formę tych konkretnych postanowień w porozumieniu z Head Legal & Compliance. Nie wolno jednak zmieniać treści i celu odnośnych postanowień.

4 PODSTAWY PRAWNE

Niniejsza Instrukcja dot. ochrony danych osobowych bazuje na RODO i uznanych globalnie podstawowych zasadach ochrony danych.

5 ROLE I ZAKRESY OBOWIĄZKÓW

- Dyrektor zarządzający spółki koncernu[1] jest odpowiedzialny za:
  1. ostateczne upewnianie się, że dana osoba prawna spełnia swoje zobowiązania prawne w odniesieniu do przetwarzania danych osobowych.
  2. upewnienie się, że spełniane są wymagania niniejszej Instrukcji dot. ochrony danych osobowych (łącznie z informacją w przypadku incydentów związanych z ochroną danych osobowych).
  3. upewnienie się, że „Spis czynności przetwarzania" jest uzupełniany i pielęgnowany na poziomie spółki koncernu przez właściciela procesu biznesowego.
  4. wyznaczenie formalnego lokalnego pełnomocnika ds. ochrony danych osobowych (wewnętrznego lub zewnętrznego) (w dalszej części „pełnomocnik ds. ochrony danych osobowych"), jeśli wymaga tego lokalnie obowiązujące rozporządzenie ds. ochrony danych osobowych, oraz za coroczne, śródroczne informowanie o tej wyznaczonej osobie Head Legal & Compliance oraz audytu wewnętrzny.
  5. wyznaczenie lokalnego menedżera ds. ochrony danych osobowych (w dalszej części „koordynator ds. ochrony danych osobowych"), jeśli lokalnie obowiązujące rozporządzenie ds. ochrony danych osobowych nie wymaga wyznaczenia lokalnego pełnomocnika ds. ochrony danych osobowych. O wyznaczonej osobie należy corocznie, śródrocznie informować Head Legal & Compliance oraz audyt wewnętrzny.

- Wyznaczony[2] przez dyrektora zarządzającego spółki koncernu lokalny koordynator ds. ochrony danych osobowych lub pełnomocnik ds. ochrony danych osobowych odpowiada za:
  1. monitorowanie przestrzegania niniejszej Instrukcji dot. ochrony danych osobowych i instrukcji podmiotu odpowiedzialnego za przetwarzanie danych osobowych bądź podmiotu przetwarzającego zlecenie związanych z ochroną danych osobowych, łącznie z transferem zakresu obowiązków i odpowiednimi kontrolami.
  2. informowanie, udzielanie porad i monitorowanie podmiotu odpowiedzialnego za przetwarzanie danych osobowych lub podmiotu przetwarzającego zlecenie oraz osób zatrudnionych w kwestiach związanych z niniejszą Instrukcją dot. ochrony danych osobowych.

[1] Dla spółek koncernu, które działają operacyjnie, odpowiedzialność ta jest uzgadniana oddzielnie w porozumieniu z Head Legal & Compliance.
[2] Dla spółek koncernu, które działają operacyjnie, odpowiedzialność ta jest uzgadniana oddzielnie w porozumieniu z Head Legal & Compliance.

3. na żądanie udzielanie porad dotyczących szacowania skutków dla ochrony danych osobowych oraz monitorowanie jej wyników oraz odpowiadanie na inne pytania dotyczące danych osobowych, które są do niego przypisane zgodnie z niniejszą Instrukcją dot. ochrony danych osobowych.
4. upewnianie się, że „Spis czynności przetwarzania", prowadzony przez daną spółkę koncernu i wypełniany przez właściciela procesu biznesowego jest zawsze utrzymywany w aktualnym stanie oraz coroczne śródroczne potwierdzanie wobec dyrektora zarządzającego oraz Head Legal & Compliance kompletności i aktualności listy.
5. działanie jako osoba kontaktowa Head Legal & Compliance i informowanie go na bieżąco o odpowiedzialności, ryzyku i problemach związanych z ochroną danych osobowych.
6. wspieranie od strony bezpieczeństwa danych odpowiedzialnego za zastosowania IT działu IT w kontroli i zezwalaniu na nowe zastosowania IT na poziomie spółki koncernu, związane z przetwarzaniem danych osobowych oraz na każde zastosowanie IT związane z przetwarzaniem szczególnych kategorii danych osobowych.
7. zezwalanie na przekazywanie danych osobowych do krajów trzecich pod kątem ochrony danych (por. dalej, pkt. 14).
8. działanie jako lokalny podmiot kontaktowy dla urzędu nadzorczego w kwestii pytań związanych z przetwarzaniem danych osobowych oraz współpraca z urzędem nadzorczym,
9. odpowiadanie na zapytania osób zatrudnionych zajmujących się przetwarzaniem danych osobowych.
10. odpowiadanie na zapytania osób, których dane dotyczą, dotyczące informacji na temat ich danych osobowych przechowywanych przez firmę Arbonia, lub w przypadku zapytania skierowanego do więcej niż jednej spółki koncernu Arbonia odpowiadanie na nie współpracy z działem Corporate IT (por. dalej, pkt. 7.4)
11. sprawdzanie i zatwierdzanie opracowanych lub wstępnie zatwierdzonych przez właściciela procesu biznesowego umów lub porozumień z podmiotem przetwarzającym zlecenie, które mogą obejmować przetwarzanie danych osobowych na zlecenie Arbonia, jak to opisano w rozdziale 7.2.
12. nadzorowanie zewnętrznego lokalnego pełnomocnika ds. ochrony danych osobowych, jeśli został on wyznaczony.
13. zgłaszanie incydentów związanych z ochroną danych zgodnie z instrukcją Data Breach Notification (por. dalej, pkt. 9 oraz „Arbonia Data Breach Policy").

■ IT-Board w porozumieniu z Corporate IT odpowiada za:

1. zdefiniowanie obowiązujących dla całego koncernu standardu oraz IT Controls (GITC), których należy przestrzegać przy zapisywaniu danych.

■ Odpowiedni dział IT, zarządzany przez spółkę koncernu, odpowiada za:

1. upewnianie się za pomocą odpowiednich standardów, polityki i przeprowadzania ogólnych kontroli IT (GITC), że systemy, usługi i wyposażenie używane do

zapisywania danych spełniają odpowiednie standardy bezpieczeństwa (kontrola dostępu/usuwanie danych), przy czym należy uwzględnić stan techniki, koszty realizacji oraz rodzaj, zakres, związek i cel przetwarzania danych oraz różne możliwości i stopień oddziaływania na prawa i swobody osób fizycznych.

2. dążenie do tego, aby podmiot odpowiedzialny za przetwarzanie danych osobowych i podmiot przetwarzający zlecenie stosowały odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom ochrony odpowiedni do ryzyka, jak to opisano w rozdziale 8.
3. po konsultacji z koordynatorem lub pełnomocnikiem ds. ochrony danych osobowych sprawdzanie i zatwierdzanie nowych środków IT do przetwarzania danych osobowych pod kątem ochrony danych osobowych.
4. przeprowadzanie regularnych kontroli i skanowania, aby upewniać się, że sprzęt i oprogramowanie związane z bezpieczeństwem działają prawidłowo. Wyniki kontroli danych osobowych należy zgłaszać odpowiedzialnemu pełnomocnikowi ds. ochrony danych osobowych.
5. ocena bezpieczeństwa danych wszystkich zewnętrznych dostawców usług (np. podmiotów przetwarzających zlecenia), które przedsiębiorstwo angażuje w przetwarzanie danych osobowych (np. w kwestii usług Cloud Computing itd.)
6. tworzenie listy incydentów związanych z bezpieczeństwem danych i zgłaszanie takich incydentów do Corporate IT.
7. koordynowanie oraz odpowiadanie na zapytania osób, których dane dotyczą, dotyczące informacji na temat ich danych osobowych przechowywanych przez obsługiwaną przez dany dział IT spółkę koncernu Arbonia (por. dalej, pkt. 7.4)
8. zgłaszanie wykrytych incydentów lub zagrożeń związanych z ochroną danych zgodnie z instrukcją Data Breach Notification (por. dalej, pkt. 9 oraz „Arbonia Data Breach Policy")

- Corporate IT we współpracy z działem IT odpowiedzialnym za daną spółkę koncernu: Są odpowiedzialne za
  1. przeprowadzanie regularnych kontroli i skanowania, aby upewniać się, że sprzęt i oprogramowanie związane z bezpieczeństwem działają prawidłowo. Wyniki kontroli danych osobowych należy zgłaszać odpowiedzialnemu pełnomocnikowi ds. ochrony danych osobowych.
  2. tworzenie centralnej listy incydentów związanych z bezpieczeństwem danych.
  3. zgłaszanie wykrytych incydentów lub zagrożeń związanych z ochroną danych zgodnie z instrukcją Data Breach Notification (por. dalej, pkt. 9 oraz „Arbonia Data Breach Policy").

- Internal Audit jest odpowiedzialny za:
  1. przy okazji audytu zgodnego z wymogami planowania audytów sprawdzanie w ramach kontroli ryzyka, czy procedury organizacyjne są zgodne z istotnymi wymogami niniejszej Instrukcji dot. ochrony danych osobowych.

- Właściciel procesu biznesowego jest odpowiedzialny za:

1. upewnienie się, że lokalny pełnomocnik ds. ochrony danych osobowych odpowiednio i na czas jest angażowany we wszystkie kwestie wymagane do oceny przetwarzania danych osobowych.
2. opracowywanie lub wstępne zatwierdzanie wszystkich umów i porozumień z podmiotem przetwarzającym zlecenie, które mogą obejmować przetwarzanie danych osobowych na zlecenie Arbonia, jak to opisano w rozdziale 7.2
3. wypełnianie i aktualizowanie „spisu czynności przetwarzania" prowadzonego przez daną spółkę koncernu i corocznie, do końca kwietnia, potwierdzanie kompletności i aktualności wpisów wobec koordynatora wzgl. pełnomocnika ds. ochrony danych osobowych.
4. przed zaimplementowaniem nowych procedur przetwarzania danych osobowych ocenę wynikającego z nich ryzyka dla osoby, której dane dotyczą i jej podstawowych praw, a przy przewidywanym wysokim ryzyku przetwarzania wykonanie przed nim szacowania skutków dla ochrony danych osobowych.

6 PODSTAWY OCHRONY DANYCH OSOBOWYCH DLA PRZETWARZANIA DANYCH OSOBOWYCH

Każda spółka koncernu działająca jako podmiot odpowiedzialny za przetwarzanie danych osobowych musi się upewnić, że możliwe jest **udowodnienie przestrzegania poniższych 6 (sześciu) podstaw ochrony danych osobowych:**

1. Dane osobowe są przetwarzane wyłącznie, gdy można udowodnić istnienie ku temu obowiązującej podstawy prawnej zgodnie z obowiązującymi przepisami danych osobowych i gdy osoba, której dane dotyczą, została poinformowana o tożsamości i danych kontaktowych podmiotu odpowiedzialnego za przetwarzanie danych, rodzaju gromadzonych danych osobowych i podstawach prawnych ich gromadzenia, okresach przechowywania danych i celu, w jakim dane są gromadzone

2. Zawsze przestrzegany jest cel, w jakim dane osobowe zostały zgromadzone

3. Rejestrowane i przetwarzane są wyłącznie faktycznie wymagane dane osobowe

4. Utrzymywany jest prawidłowy stan danych osobowych, nieprawidłowe dane są usuwane

5. Dane osobowe są przechowywane jedynie przez faktycznie konieczny i zgodny z prawem czas

6. Dane osobowe są traktowane w sposób poufny i udostępniane tylko, gdy jest to rzeczywiście konieczne

6.1 Uczciwość, zgodność z prawem i transparentność

Dane osobowe wolno przetwarzać wyłącznie w celach, które są dozwolone, jak to opisano poniżej; musi się to odbywać w sposób transparentny. Dane osobowe należy przy tym przetwarzać w zgodny z prawem i uczciwy sposób, przestrzegając indywidualnych praw osób, których dane dotyczą. Może to obejmować dane osobowe, które koncern Arbonia otrzymuje bezpośrednio od osoby, której dane dotyczą (np. poprzez wypełnianie formularzy lub korespondencję z nami drogą pocztową, telefoniczną lub mailową), a także dane osobowe otrzymane przez koncern Arbonia od stron trzecich.

W świetle obowiązujących ustaw dotyczących ochrony danych osobowych, dane osobowe mogą być zgodnie z prawem przetwarzane na jednej z **pięciu zgodnych z prawem podstaw** (**podstawy zgodne z prawem**), zgodnie z RODO. Podstawy te są następujące:

1. **Umowa:** przetwarzanie danych osobowych jest wymagane do realizacji umowy, w której stroną jest osoba, której dane dotyczą, bądź do realizacji środków przedumownych na żądanie osoby której dane dotyczą;

2. **Wyrażenie zgody:** przetwarzanie danych osobowych bazuje na wyrażeniu na nie zgody przez osobę, której dane dotyczą (model opt-in), dla jednego lub więcej specyficznych celów. Wyrażenie zgody musi być udokumentowane;

3. **Zobowiązanie prawne:** przetwarzanie danych osobowych wynika ze zobowiązania prawnego koncernu Arbonia. Rodzaj i zakres przetwarzania danych muszą być niezbędne do zgodnej z prawem czynności przetwarzania i obejmować obowiązujące warunki ustawowe;

4. **Interes publiczny:** przetwarzanie danych jest niezbędne do wykonania zadania leżącego w interesie publicznym;

5. **Uprawniony interes biznesowy:** przetwarzanie jest w stosownym zakresie wymagane dla uprawnionego interesu biznesowego Arbonia lub stron trzecich, którym udostępniono dane osobowe, poza przypadkami, gdy podstawowe prawa bądź wolności osoby, której dane dotyczą, przeważają nad takim interesem. Uprawniony interes może być prawny (np. odzyskanie istniejących długów / przez zbiorowy układ pracy z radą zakładową / dochodzenie/realizacja roszczeń prawnych bądź obrona przed roszczeniami prawnymi względem osoby, której dane dotyczą) bądź komercyjny (np. unikanie naruszeń umowy).

Transparencja wymaga, aby osoba, której dane dotyczą, została poinformowania o przetwarzaniu jej danych. Ogólnie zaleca się, aby dane osobowe pozyskiwać bezpośrednio od osoby, której dotyczą (nie za pośrednictwem osób trzecich). Jeśli dane osobowe są przetwarzane, należy udzielić osobie, której dane dotyczą, następujących informacji:

- nazwy i dane kontaktowe podmiotów odpowiedzialnych za przetwarzanie danych osobowych oraz, w razie potrzeby, ich przedstawiciel na terenie UE
- w razie potrzeby dane kontaktowe koordynatora lub pełnomocnika ds. ochrony danych osobowych
- cel oraz podstawa prawna przetwarzania danych osobowych,
- odbiorcy będący stronami trzecimi lub kategorie odbiorców będących stronami trzecimi, którym mogą być przekazywane dane
- jeśli mają zastosowanie, informacje na temat przetwarzania danych w krajach trzecich w wskazanie odpowiednich gwarancji bezpieczeństwa

6.2 Cel wykorzystywania

Dane osobowe mogą być przetwarzane wyłącznie w celu, o którym osoba, której dane dotyczą, została poinformowana w momencie zbierania danych. Późniejsze zmiany celu są możliwe tylko w ograniczonym zakresie i wymagają uzasadnienia. Podmiot odpowiedzialny za przetwarzanie danych osobowych musi poinformować osobę, której dane dotyczą o celu, w jakim Arbonia przetwarza jej dane osobowe, w momencie, gdy Arbonia gromadzi te dane lub możliwie najszybciej po ich zgromadzeniu. Przy każdym przetwarzaniu dla celów reklamowych lub programów marketingowych należy udzielić osobie, której dane dotyczą, prawa do sprzeciwu wobec przetwarzania jej danych osobowych i musi ona zostać o tym wyraźnie poinformowana. W szczególności każdy podmiot odpowiedzialny za przetwarzanie danych osobowych musi realizować przetwarzanie skarg w sposób, który zapewnia opcję opt-out.

6.3 Minimalizacja danych

Należy przetwarzać tylko dane osobowe, które są faktycznie wymagane. Przed przetwarzaniem danych osobowych należy określić, czy i jaki zakres przetwarzania danych jest konieczny do osiągnięcia celu, w jakim przetwarzanie się odbywa. Danych osobowych nie wolno rejestrować z wyprzedzeniem ani zapisywać do potencjalnych przyszłych celów, jeżeli nie wymaga ani nie dozwala tego obowiązujące prawo krajowe.

6.4 Prawidłowe i aktualne

Dane osobowe muszą być zawsze prawidłowe, kompletne i – jeśli dokonywano ich zmian – zaktualizowane. Należy podjąć stosowne kroki w celu zapewnienia, że nieprawidłowe lub niekompletne dane osobowe będą usuwane, poprawiane, uzupełniane lub aktualizowane. Wszystkie osoby pracujące z danymi osobowymi zawsze muszą podejmować w tym celu odpowiednie środki (przykładowo poprzez potwierdzanie danych osoby, której one dotyczą, gdy kontaktuje się ona z nami telefonicznie, lub usuwanie numeru telefonu z bazy danych, gdy osoba, której dane dotyczą, przestanie z niego korzystać).

6.5 Ograniczony czas przechowywania

Dane osobowe można przechowywać tylko przez faktycznie wymagany czas. Dane osobowe należy usunąć, gdy nie są już wymagane do przewidzianych celów, gdy zgoda zostanie wycofana lub gdy zostanie wyrażony sprzeciw wobec przetwarzania na podstawie uprawnionego interesu, a koncern Arbonia nie potrafi podać nadrzędnego uprawnionego powodu. W pewnych przypadkach dłuższe okresy przechowywania mogą dozwalać przechowywanie przez nas danych przez dłuższy czas, jeśli jest to wymagane prawnie (np. przez ustawy podatkowe i handlowe) lub gdy dane osobowe są wymagane do dochodzenia, realizacji i obrony roszczeń prawnych.

6.6 Poufność i bezpieczeństwo danych

Dane osobowe należy zawsze traktować w sposób poufny i udostępniać je tylko, gdy jest to rzeczywiście konieczne. Obowiązuje podstawowa zasada „wymagana informacja", tak, że pracownicy i strony trzecie otrzymują dostęp do danych wyłącznie gdy są one wymagane do realizacji celu i tylko w wymaganym do tego zakresie. Wymaga to starannie utworzonej koncepcji, która definiuje specyficzne uprawnienia dostępu dla każdego procesu biznesowego, łącznie z przydzielaniem i zatwierdzaniem ról i zakresów obowiązków (koncepcja uprawnień dostępu). Odbiorców danych osobowych należy poinformować o poufności danych osobowych i **muszą oni zatwierdzić porozumienie o zachowaniu poufności/o tajności** (które może być częścią umowy o pracę lub mieć podobną formę). Wyjątek: nie jest to konieczne, gdy odbiorca podlega obowiązkowi tajemnicy zawodowej lub ustawowej.

Dane osobowe należy zabezpieczyć za pomocą odpowiednich środków organizacyjnych i technicznych, aby zapobiegać nieprawidłowemu dostępowi, niezgodnemu z prawem przetwarzaniu lub publikacji oraz przypadkowej utracie, zmianom i zniszczeniu danych (por. pkt. 8).

7 DALSZE OBOWIĄZKI WYNIKAJĄCE Z RODO LUB INNYCH PODOBNYCH ROZPORZĄDZEŃ DOT. OCHRONY DANYCH OSOBOWYCH

7.1 Podstawa – obowiązek rozliczalności

Spółka koncernu Arbonia podlegająca RODO (lub innemu obowiązującemu rozporządzeniu dot. ochrony danych osobowych) musi być w stanie udowodnić przestrzeganie obowiązujących przepisów ochrony danych (podstawa „obowiązek rozliczalności"). W tym celu spółki koncernu muszą, oprócz ogólnych wymagań niniejszej Instrukcji dot. ochrony danych osobowych, realizować i spełniać poniższe punkty, przy czym dyrektor zarządzający danej spółki koncernu ostatecznie zapewnia realizację i spełnianie:

1. Lokalny koordynator ds. ochrony danych osobowych lub lokalny pełnomocnik ds. ochrony danych osobowych: Wyznaczenie specjalnego lokalnego koordynatora bądź pełnomocnika ds. ochrony danych osobowych

2. Prowadzenie „spisu czynności przetwarzania": Należy prowadzić i aktualizować spis czynności związanych z przetwarzaniem danych osobowych.

3. Kontrola zgodności z prawem: Należy sprawdzić zgodność z prawem przetwarzania danych osobowych przy zachowaniu obowiązującej zgodnej z prawem podstawy, zwłaszcza przy przetwarzaniu szczególnych kategorii danych osobowych

4. Kontrola podmiotu przetwarzającego dane: Zawarcie umowy na przetwarzanie danych z podmiotem przetwarzającym dane lub jako podmiot przetwarzający dane przy dostarczaniu lub odbiorze danych osobowych zgodnie z dopuszczeniem według Art. 28 RODO.

5. W przypadku podmiotów współodpowiedzialnych za przetwarzanie danych osobowych należy przewidzieć zawarcie umowy między podmiotami współodpowiedzialnymi za przetwarzanie danych osobowych, zgodnie z Art. 26 RODO.

6. Pracowników koncernu Arbonia należy informować o czynności przetwarzania danych osobowych.

7.2 Reguły dla podmiotów przetwarzających zlecenie (przede wszystkim partnerów w zakresie usług)

Podmiot odpowiedzialny za przetwarzanie danych osobowych współpracuje tylko podmiotami przetwarzającymi zlecenia, które zapewniają wystarczające gwarancje stosowania środków technicznych i organizacyjnych zgodnych z wymaganiami art. 28 RODO i gwarantujących ochronę praw osoby, której dane dotyczą.

Dla wykonywanych usług wewnątrz koncernu Arbonia istnieje porozumienie, które dozwala na przekazywanie danych osobowych, jeżeli istnieją wystarczające przyczyny prawne dla przekazania tych danych osobowych zgodnie z obowiązującymi ustawami dotyczącymi ochrony danych osobowych.

7.2.1 Udostępnianie danych osobowych podmiotowi przetwarzającemu zlecenie (wychodzące)

Przetwarzanie danych osobowych za zezwoleniem oznacza, że usługodawca otrzymuje zlecenie na przetwarzanie danych osobowych, ale nie jest na niego przenoszona odpowiedzialność za dany proces biznesowy (np. usługodawca, outsourcing usług). W takim wypadku należy zawrzeć z zewnętrznym dostawcą umowę na przetwarzanie danych osobowych za zezwoleniem. Każda spółka koncernu Arbonia jest podmiotem odpowiedzialnym za przetwarzanie danych osobowych i zachowuje pełną odpowiedzialność za prawidłowe wykonywanie przetwarzania danych osobowych przez podmiot przetwarzający zlecenie.

Dany właściciel procesu biznesowego musi zapewnić, że stosowane będzie aktualne porozumienie wzorcowe na przetwarzanie zleceń lub odpowiednie podobne porozumienie przygotowane przez usługodawcę w celu spełnienia wymagań Art. 28 RODO, aby mógł zatrudnić takiego usługodawcę. Alternatywnie usługodawca może udokumentować swoje przestrzeganie wymogów bezpieczeństwa danych, przedkładając stosowną i zatwierdzoną certyfikację UE. Każde odchylenie od takiego standardu bezpieczeństwa musi zostać zatwierdzone przez pełnomocnika wzgl. koordynatora ds. ochrony danych osobowych we współpracy z działem Corporate IT. Istniejące umowy należy zmodyfikować w ciągu roku od wejścia w życie niniejszej Instrukcji dot. ochrony danych osobowych, musi być dostępna pisemna umowa o przetwarzaniu zlecenia.

7.2.2 Odbiór danych osobowych jako podmiot przetwarzający zlecenie (przychodzące)

Jeśli dane osobowe są przekazywane spółce koncernu Arbonia przez stronę trzecią należy upewnić się, że dane osobowe (i) mogą być stosowane do przewidzianego celu, (ii) zostały zgromadzone w oparciu o zgodną z prawem podstawę (zalecane jest uzyskanie pisemnego potwierdzenia) oraz (iii) istnieje umowa na przetwarzanie danych osobowych zgodna z Art. 28 RODO.

7.3 Przekazywanie danych osobowych do innych państw

W przypadku przekazywania danych osobowych do innych państw muszą być spełnione obowiązujące krajowe wymagania dotyczące publikacji danych osobowych za granicą. Zgodnie z przepisami RODO, dane osobowe mogą być przekazywane w obrębie UE, EOG lub do krajów, co do których Komisja Europejska stwierdziła, że zapewniają one odpowiednie gwarancje dla zapewnienia stosownego poziomu ochrony danych osobowych. Takie przekazywanie danych osobowych nie wymaga oddzielnej zgody. Komisja Europejska wymienia m.in. Szwajcarię jako kraj o odpowiednim poziomie ochrony danych osobowych (por. aktualna lista państw:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Przekazywanie danych osobowych do krajów trzecich jest dozwolone wyłącznie, gdy istnieją dodatkowe, odpowiednie gwarancje. Wymagają one, aby odbiorca danych udowodnił, że stosuje standard ochrony danych odpowiadający niniejszej Instrukcji dot. danych osobowych (np. i) istnieją wiążące reguły przedsiębiorstwa, ii) z usługodawcą i innymi podwykonawcami zostały zawarte standardowe klauzule umowne UE dla przetwarzania zleceń w krajach trzecich [3], iii) są stosowane reguły postępowania zatwierdzone przez urząd nadzorczy, iv) w przypadku uczestnictwa usługodawcy w akredytowanym przez UE systemie certyfikacji, dla osiągnięcia wystarczającego poziomu danych osobowych lub v) dla pojedynczych porozumień między podmiotem odpowiedzialnym za przetwarzanie danych osobowych a podmiotem przetwarzającym zlecenie, za zezwoleniem odpowiedniego urzędu nadzorczego), a także poinformowania osoby, której dane dotyczą. Nie ma tego obowiązku, gdy przekazanie następuje na podstawie prawnej. Takie przekazanie wymaga zezwolenia koordynatora lub pełnomocnika ds. ochrony danych osobowych.

Jeśli dane osobowe są przekazywane wewnątrz koncernu Arbonia, spółka koncernu importująca dane osobowe jest zobowiązana współpracować w sprawie wszelkich zapytań kierowanych przez odpowiedzialne urzędy nadzorcze w kraju, w którym mieści się zarejestrowana siedziba eksportującej dane spółki koncernu, a także odpowiadać na wszystkie uwagi urzędów nadzorczych dotyczące przetwarzania przekazanych danych osobowych.

7.4 Postępowanie z zapytaniami o informacje osób, których dane dotyczą.

Osoby, których dane dotyczą, mają prawo zadawać formalne zapytania o informacje dotyczące szczegółów ich danych osobowych, które posiada Arbonia, i mogą zgłaszać następujące żądania:

Prawo do informacji na temat:

- celów przetwarzania danych;
- kategorii danych osobowych, które przetwarzamy;
- odbiorców lub grup odbiorców, którym udostępnione zostały lub udostępniane są dane osobowe, w szczególności odbiorców z krajów trzecich lub będących organizacjami międzynarodowymi;
- jeśli to możliwe, planowanego czasu przechowywania danych osobowych lub, jeśli nie jest to możliwe, kryteriów dla określenia tego czasu.
- istnienia prawa do sprostowania lub usunięcia odpowiednich danych osobowych bądź ograniczenia ich przetwarzania przez podmiot odpowiedzialny za przetwarzanie danych, bądź wyrażenia sprzeciwu wobec takiego przetwarzania;
- istnienia prawa do złożenia skargi w urzędzie nadzorczym;

[3] Por. Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

- wszystkich dostępnych informacji na temat źródeł danych osobowych, jeśli nie zostały one otrzymane od osoby, której dane dotyczą;
- istnienia zautomatyzowanych procesów decyzyjnych, łącznie z profilowaniem;
- Jeśli dane osobowe są przekazywane do krajów trzecich lub organizacji międzynarodowych, osoba, której dane dotyczą, ma prawo do informacji o istniejących gwarancjach.

Prawo do sprostowania:

- Osoba, której dane dotyczą, ma prawo zażądać niezwłocznego sprostowania przez podmiot odpowiedzialny za przetwarzanie danych osobowych jej błędnych danych osobowych. Przy uwzględnieniu celów przetwarzania danych osobowych osoba, której dane dotyczą, ma prawo do żądania uzupełnienia swoich niekompletnych danych osobowych, również poprzez deklarację uzupełniającą.

Prawo do usunięcia („Prawo do bycia zapomnianym"):

- Osoba, której dane dotyczą, ma prawo zażądać od podmiotu odpowiedzialnego za przetwarzanie danych osobowych niezwłocznego usunięcia dotyczących jej danych, a podmiot odpowiedzialny za przetwarzanie ma obowiązek niezwłocznie je usunąć, jeżeli spełniony jest jeden z poniższych warunków:
  1. Dane osobowe nie są już wymagane do celów, w których zostały oryginalnie zapisane lub w inny sposób przetworzone;
  2. Osoba, której dane dotyczą, wycofa swoją zgodę, która była podstawą przetwarzania zgodnie z Art. 6 ust. 1 lit. a RODO lub Art. 9 ust. 2 lit. a RODO, i nie istnieje inna podstawa prawna przetwarzania danych;
  3. Osoba, której dane dotyczą, zgłosi sprzeciw wobec ich przetwarzania zgodnie z art. 21 ust. 1 RODO i nie istnieją nadrzędne, uzasadnione powody dla ich przetwarzania, lub osoba, której dane dotyczą, zgłosi sprzeciw wobec ich przetwarzania zgodnie z Art. 21 ust. 2 RODO;
  4. Dane osobowe były przetwarzane w sposób niezgodny z prawem;
  5. Usunięcie danych osobowych jest wymagane dla spełnienia wymogu prawnego zgodnie z prawem danego kraju członkowskiego, któremu podlega podmiot odpowiedzialny za przetwarzanie danych osobowych;
  6. Dane osobowe są przetwarzane w odniesieniu do oferowanych usług społeczeństwa informacyjnego zgodnie z Art. 8, ust. 1 RODO.

Prawo do ograniczenia przetwarzania:

- Osoba, której dane dotyczą, ma prawo zażądać od podmiotu odpowiedzialnego za przetwarzanie danych osobowych ograniczenia przetwarzania, jeśli spełniony jest jeden z poniższych warunków:
- jeśli prawidłowość danych osobowych jest kwestionowana przez osobę, której dane dotyczą, przez czas umożliwiający podmiotowi odpowiedzialnemu za przetwarzanie danych osobowych sprawdzenie ich prawidłowości;

- jeśli przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, nie zgadza się na ich usunięcie i zamiast tego wymaga ograniczenia przetwarzania danych osobowych;
- jeśli podmiot odpowiedzialny za przetwarzanie danych osobowych nie wymaga już danych do celów ich przetwarzania, jednak osoba, której dane dotyczą, wymaga ich do dochodzenia, realizacji lub obrony roszczeń prawnych,
- jeśli osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania danych osobowych zgodnie z Art. 21 ust. 1, o ile nie stwierdzono jeszcze, czy uzasadniony interes podmiotu odpowiedzialnego za przetwarzanie danych osobowych przeważa nad interesem osoby, której dane dotyczą.

Osobę, której dane dotyczą, należy poprosić o sformułowanie swojego żądania w formie pisemnej i przesłania go e-mailem lub pocztą do odpowiedniego lokalnego pełnomocnika ds. ochrony danych osobowych. Informacje są przekazywane osobie, której dane dotyczą, przez lokalnego pełnomocnika ds. ochrony danych osobowych, niezwłocznie, jednak w żadnym wypadku nie później niż w ciągu miesiąca od nadejścia zapytania. Termin ten może ulec przedłużeniu o dalsze dwa miesiące, jeśli jest to konieczne ze względu na złożoność i liczbę zapytań. Koordynator lub pełnomocnik ds. ochrony danych osobowych podmiotu odpowiedzialnego za przetwarzanie danych osobowych w ciągu miesiąca od wpłynięcia zapytania informuje osobę, której dane dotyczą, o przedłużeniu terminu, podając przyczyny opóźnienia. Nie wolno obciążać osoby, której dane dotyczą, kosztami wynikającymi z żądania informacji o danych, jakie posiada na jej temat spółka koncernu Arbonia, chyba że żądania osoby, której dane dotyczą, są w wyraźny sposób nieuzasadnione lub przesadne, zwłaszcza ze względu na powtarzane ich zgłaszanie. Zapytania osoby, której dane dotyczą, kierowane do kilku spółek koncernu Arbonia, należy przekazywać w celu koordynacji i udzielania odpowiedzi działowi Corporate IT.

7.5 Przeprowadzanie szacowania skutków dla ochrony danych osobowych

Jeśli planowana nowa forma przetwarzania danych osobowych, w szczególności z użyciem nowych technologii, może ze względu na rodzaj, zakres, okoliczności i cele przetwarzania przypuszczalnie stwarzać wysokie ryzyko dla praw i wolności osób, których dane dotyczą, należy z wyprzedzeniem przeprowadzić oszacowanie skutków planowanych procesów przetwarzania dla ochrony danych osobowych.

Dlatego przed zaimplementowaniem nowych procedur przetwarzania należy przeprowadzić ocenę wynikającego z nich ryzyka dla osoby, której dane dotyczą i jej podstawowych praw. W przypadku nowych zastosowań IT należy dokonać tego w ramach procesu udzielania zezwolenia. Jeśli pierwsze szacowanie wykaże, że planowana nowa forma przetwarzania danych osobowych możne stwarzać wysokie ryzyko dla osób, których dane dotyczą, należy przeprowadzić szacowanie skutków dla ochrony danych osobowych.

Zapytania na temat konieczności lub zapytania podczas przeprowadzania szacowania skutków dla ochrony danych osobowych należy kierować do lokalnego koordynatora wzgl.

pełnomocnika ds. ochrony danych osobowych. Po przeprowadzeniu szacowania skutków dla ochrony danych osobowych należy poinformować lokalnego koordynatora wzgl. pełnomocnika ds. ochrony danych osobowych i uzyskać jego stanowisko.

Jeśli z szacowania skutków dla ochrony danych osobowych wynika, że przetwarzanie niosłoby ze sobą wysokie ryzyko dla osób, których dane dotyczą, i nie zostały podjęte żadne środki w celu minimalizacji ryzyka, przed zaimplementowaniem nowych procesów przetwarzania należy skonsultować się z urzędem nadzorczym.

8 BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Dane osobowe muszą być chronione przed niepowołanym dostępem, przetwarzaniem i publikacją oraz przypadkową utratą, zmianą lub zniszczeniem. Wymóg ten obowiązuje niezależnie od tego, czy dane osobowe są przetwarzane w formie elektronicznej, czy papierowej.

Podmiot odpowiedzialny za przetwarzanie danych osobowych i podmiot przetwarzający zlecenie muszą stosować odpowiednie środki techniczne i organizacyjne, aby zabezpieczyć dane osobowe przed nieuprawnionym przetwarzaniem. Środki te muszą bazować na (i) uznanych procedurach, (ii) ryzyku związanym z przetwarzaniem oraz (iii) konieczności ochrony danych osobowych (zwłaszcza w trakcie procesów w celu klasyfikacji informacji); obejmują one między innymi następujące środki, jeśli dotyczy:

(a) pseudonimizacja i szyfrowanie danych osobowych;

(b) zapewnienie trwałej dostępności, poufności, integralności, dostępności i przepustowości systemów i usług związanych z przetwarzaniem danych;

(c) możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie awarii fizycznej lub technicznej;

(d) procedura w celu regularnego sprawdzania, analizy i ewaluacji skuteczności środków technicznych i organizacyjnych służących zagwarantowaniu bezpieczeństwa przetwarzania danych.

Środki techniczne i organizacyjne w celu ochrony danych osobowych są częścią wewnętrznego zarządzania bezpieczeństwem danych i muszą stale być dopasowywane do rozwoju technicznego i zmian organizacyjnych.

Procedury bezpieczeństwa muszą obejmować co najmniej:

- Kontrole dostępu: należy zgłaszać każdą osobę z zewnątrz, która znajdzie się w obszarach podlegających kontroli dostępu.

- Bezpiecznie zamykane szuflady lub szafki na akta: biurka i szafki zawierające poufne dokumenty powinny pozostawać bezpiecznie zamknięte. Dane osobowe zawsze uważane są za informacje poufne. Pracownicy muszą się upewnić, że dokumenty i wydruki zawierające dane osobowe nie są pozostawiane w ogólnodostępnych miejscach, np. w drukarce. Jeśli dane osobowe są za pozwoleniem zapisywane na nośniku wymiany danych (np. CD, pamięć USB, DVD), nośnik ten należy przechowywać bezpiecznie zamknięty, gdy nie jest używany.
- Metody utylizacji: dokumenty w formie papierowej należy zniszczyć za pomocą niszczarki i bezpiecznie zutylizować, gdy nie są już wymagane. Dotyczy to również danych osobowych, które są zasadniczo przechowywane w formie elektronicznej, zostały jednak wydrukowane.

- Dane zapisane w formie elektronicznej: dane osobowe powinny być chronione hasłami zgodnymi z obecną dyrektywą dotyczącą haseł i nigdy nie mogą być przekazywane między osobami zatrudnionymi. Dane w formie elektronicznej muszą być zapisywane na serwerach systemów IT i w ustrukturyzowanych systemach informatycznych i z nich wywoływane; nie mogą być przechowywane w formie niezaszyfrowanej na lokalnych komputerach.

- Dane osobowe pozyskane w formie elektronicznej, przekazane przez osobę, której dane dotyczą: należy sprawdzić tożsamość osoby, której dane dotyczą; preferowaną metodą jest proces podwójnego opt-in (druga wiadomość e-mail w celu weryfikacji podanego adresu e-mail). Jeśli dostęp do strony internetowej lub aplikacji jest ograniczony do zarejestrowanych użytkowników (tzn. kont użytkownika), identyfikacja i uwierzytelnianie osoby, której dane dotyczą, musi oferować odpowiedni poziom bezpieczeństwa, adekwatny do treści widocznych podczas dostępu.

- Zachowanie ostrożności przy udostępnianiu danych osobowych: nigdy nie wolno nieformalnie udostępniać danych osobowych. Obowiązuje podstawa „wymagane informacje". Obowiązuje koncepcja separacji i podziału dla każdego procesu biznesowego oraz stosowanie ról i zakresów obowiązków. Dane osobowe przed przekazaniem w formie elektronicznej należy zaszyfrować. Menedżer technologii informacyjnych może wyjaśnić, w jaki sposób dane osobowe są przesyłane do autoryzowanych zewnętrznych osób kontaktowych.

- Otrzymywanie instrukcji: w razie pytań lub wątpliwości dotyczących aspektów ochrony danych osobowych lub istniejących obowiązków wynikających z niniejszej Instrukcji dot. ochrony danych osobowych należy zasięgnąć rady u bezpośredniego przełożonego, lokalnego pełnomocnika ds. ochrony danych osobowych lub działu Legal & Compliance.

RODO wymaga, aby najszybciej, jak to możliwe, uwzględnić sferę prywatną. Sfera prywatna w związku z aranżacją techniczna wymaga, aby uwzględnić organizacje sfery prywatnej w pierwszych stopniach aranżacji technicznej i podczas całego procesu rozwoju nowych produktów, procedur i usług związanych z przetwarzaniem danych osobowych. Prywatność jako ustawienie domyślne oznacza, że jeśli system lub usługa obejmuje decyzje poszczególnych osób na temat tego, ile swoich danych chcą one udostępnić, ustawieniem domyślnym powinno być takie, które zapewnia najwyższy możliwy stopień ochrony sfery prywatnej. Dlatego każde nowe zastosowanie IT podlega wewnętrznemu procesowi zatwierdzenia, przy czym nowe zastosowanie IT należy w ramach ewaluacji ocenić również po kątem ochrony danych osobowych.

9 ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM DANYCH

Wiele obowiązujących rozporządzeń dot. ochrony danych osobowych wymaga bezpośredniego zgłaszania ustawodawcy incydentów związanych z ochroną danych osobowych. Wymagane jest wówczas, aby wszystkie incydenty związane z bezpieczeństwem danych niezwłocznie zgłaszać odpowiedzialnemu koordynatorowi wzgl. pełnomocnikowi ds. ochrony danych osobowych, niezależnie od tego, czy dotyczą one systemu lokalnego, czy systemu koncernu; zgłoszenie następuje zgodnie z opisem w instrukcji Arbonia na temat incydentów związanych z bezpieczeństwem danych („Arbonia Data Breach Policy"). Jeśli IT stwierdzi incydenty lub ryzyka w obszarze bezpieczeństwa danych, należy je zgłosić zgodnie z instrukcją Data Breach Notification.

Celem jest przestrzeganie obowiązku zgłaszania naruszeń obowiązujących przepisów ochrony danych wynikających z właściwych przepisów ochrony danych (np. RODO wymaga, aby zgłoszenie nastąpiło w ciągu 72 godzin od wykrycia naruszenia).

W takich przypadkach należy położyć nacisk na zachowanie obowiązujących terminów powiadamiania o naruszeniach ochrony danych i niezwłocznie zastosować środku w celu zbadania incydentu i stwierdzenia, czy bezpieczeństwo danych osobowych rzeczywiście zostało naruszone. Dział Corporate IT musi prowadzić spis przypadków naruszenia bezpieczeństwa w koncernie Arbonia, aby można było przestrzegać obowiązku zgłaszania zgodnie z prawem krajowym i aby upewnić się, że stosowane są odpowiednie zasady reprezentacji, aby naruszenia można było zgłaszać w każdym czasie. Przed zgłoszeniem do krajowego urzędu należy poinformować dział Corporate IT lub Legal and Compliance koncernu.

Należy ściśle przestrzegać wszelkich dalszych instrukcji działu Corporate IT lub lokalnych działów IT.

ARBONIA

10 SKUTKI NIEPRZESTRZEGANIA

Zachowanie przepisów niniejszej Instrukcji dot. danych osobowych jest niezmiernie ważne dla koncernu Arbonia i jego publicznego wizerunku. Nieodpowiednie przetwarzanie danych osobowych lub inne naruszenia przepisów ochrony danych osobowych mogą w wielu krajach prowadzić również do postępowania karnego oraz roszczeń odszkodowawczych. W obrębie koncernu Arbonia naruszenie reguł niniejszej Instrukcji dot. ochrony danych osobowych może pociągać za sobą sankcje wynikające z ustawy lub odpowiedniej umowy (o pracę).

11 ODCHYLENIA

Odchylenia od postanowień niniejszej instrukcji i dokumentów uzupełniających są dopuszczalne jedynie po uzgodnieniu z Head of Legal & Compliance.

12 INFORMACJE

Informacji związanych z niniejszą Instrukcją dot. ochrony danych osobowych udziela Head of Legal & Compliance.

13 WEJŚCIE W ŻYCIE

Niniejsza instrukcja wchodzi w życie z dniem 17. czerwca 2020 i zastępuje Instrukcję o postępowaniu z danymi (Instrukcję dot. ochrony danych osobowych) z dnia 5, grudnia 2013.

Arbon, 16. czerwca 2020

Arbonia AG

Alexander von Witzleben
Prezes Rady Nadzorczej i CEO

Andrea Wickart
Dyrektor działu Legal & Compliance / Główny sekretarz

ARBONIA

Dokumenty uzupełniające niniejszą Instrukcję Arbonia dot. ochrony danych osobowych:

Instrukcję dot. ochrony danych osobowych uzupełniają następujące dokumenty w obowiązującym brzmieniu:

- Instrukcja na temat osób, których dane dotyczą, oraz usuwania danych
- Instrukcja na temat przypadków naruszenia ochrony danych
- Deklaracja ochrony danych osobowych dla pracowników

Niniejszy dokument jest ważny bez podpisu.