POLITYKA OCHRONY DANYCH OSOBOWYCH

BRAD Consulting Sp. z o.o.

ul. Świętokrzyska 18/315, 00-052 Warszawa

Numer KRS 0000344356 / NIP: 7010213014

Adres e-mail: biuro@bradconsulting.pl

Nr telefonu: 605 044 509

Spis treści

I WPROWADZENIE

- Niniejsza Polityka Ochrony Danych wraz z załącznikami stanowi obowiązującą w Podmiocie dokumentację w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
- Każda osoba odpowiedzialna za wdrażanie, utrzymanie lub monitorowanie zasad przetwarzania danych osobowych w Podmiocie, w szczególności przedstawiciele najwyższego kierownictwa oraz ewentualny Inspektor Ochrony Danych, mają obowiązek zapoznania się z niniejszą Polityką Ochrony Danych, obowiązek jej przestrzegania oraz egzekwowania stosowania w Podmiocie.
- Polityka Ochrony Danych wraz z załącznikami wchodzi w życie z dniem jej podpisania przez osoby uprawnione do reprezentacji Podmiotu.
- W przedmiocie spraw nieuregulowanych Polityką Ochrony Danych, zastosowanie znajdują przepisy prawa powszechnie obowiązującego.

II REJESTRY

Podmiot **prowadzi niżej wymienione rejestry**:

- Rejestr czynności przetwarzania danych osobowych – stanowiący ewidencję wykonywanych przez Podmiot czynności na danych osobowych, rozumianych jako zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.
- Rejestr kategorii czynności przetwarzania danych osobowych – stanowiący ewidencję powierzonych Podmiotowi usług, realizowanych na zlecenie administratora związanej ze zleconymi czynnościami przetwarzania.
- Rejestr naruszeń ochrony danych osobowych – stanowiący ewidencję stwierdzonych w Podmiocie naruszeń ochrony przetwarzanych danych osobowych,
- Rejestr środków ochrony danych osobowych,
- Rejestr odbiorców danych osobowych,
- Rejestr osób upoważnionych do przetwarzania danych osobowych,
- Rejestr urządzeń służących do przetwarzania danych osobowych,
- Rejestr aplikacji służących do przetwarzania danych osobowych,

Podmiot przechowuje wymienione dokumenty: w załączeniu do niniejszej Polityki Ochrony Danych.

Z komentarzem [W1]: Prowadzenie tego rejestru nie zawsze jest wymagane. Rejestr nie będzie prowadzony w przypadku, gdy Podmiot nie wykonuje powierzonych czynności przetwarzania danych osobowych.

Z komentarzem [WW2]: Taki rejestr nie występuje w RODO. Nie należy go jednak usuwać, ponieważ zgodnie z przyjętą metodologią, stanowi on wyodrębnienie istotnej części, obowiązkowego rejestru czynności i rejestru kategorii.

Z komentarzem [WW3]: Taki rejestr nie występuje w RODO. Nie należy go jednak usuwać, ponieważ zgodnie z przyjętą metodologią, stanowi on wyodrębnienie istotnej części, obowiązkowego rejestru czynności i rejestru kategorii. Doprecyzowujemy w nim konkretne nazwy i dane kontaktowe odbiorców, uprzednio wskazanych w rzeczonych rejestrach z kategorii.

Z komentarzem [WW4]: Niniejsze rejestry nie są dosłownie wymagane przez RODO. Stanowią jednak realne wdrożenie licznych, wynikających z RODO zasad, np. zasady rozliczalności.

W przypadku ich usunięcia, należy usunąć je z wykazu załączników na końcu dokumentu, a także z samych załączników.

III NARUSZENIA OCHRONY DANYCH OSOBOWYCH

- **Podmiot wdraża procedurę naruszeniową**, znajdującą się w załączniku.
- Procedura obowiązuje wszystkie osoby pracujące lub świadczące usługi w Podmiocie.
- Procedura obowiązuje w przypadku stwierdzenia naruszenia ochrony danych osobowych lub naruszenia praw lub wolności osób, których dane osobowe są przetwarzane.

Podmiot przechowuje wymienione dokumenty: w załączeniu do niniejszej Polityki Ochrony Danych.

IV OBOWIĄZKI INFORMACYJNE

- Podmiot **wdraża stosowanie obowiązków informacyjnych**, wymienionych w załączniku.
- Zabrania się przetwarzania danych osobowych bez udzielenia obowiązku informacyjnego, chyba że indywidualnie stwierdzono podstawy wyłączenia tego obowiązku w danym przypadku.

- Przechowywanie wzorów: w załączeniu do niniejszej Polityki Ochrony Danych.
- Przechowywanie udzielonych obowiązków informacyjnych: wraz z dokumentacją właściwą (np. w załączeniu do umowy).

Podmiot przechowuje:

- szablony obowiązków informacyjnych w załączeniu do niniejszej Polityki Ochrony Danych,
- udzielone obowiązki informacyjne wraz z dokumentacją właściwą (np. w załączeniu do umowy).

V UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

- Podmiot wdraża stosowanie upoważnień do przetwarzania danych osobowych,
- Zabrania się przetwarzania danych osobowych przez osoby do tego nieupoważnione.
- Upoważnienia stosuje się względem pracowników.
- Upoważnienia można stosować względem osób fizycznych trzecich, świadczących na rzez Podmiotu usługi z użyciem narzędzi Podmiotu (np. informatyk na umowie zlecenie), jednakże decyzję w tym zakresie należy podejmować indywidualnie.

Podmiot przechowuje:

- szablony upoważnień w załączeniu do niniejszej Polityki Ochrony Danych,
- udzielone upoważnienia w części B akt osobowych, a w przypadku osób niebędących pracownikami, w załączeniu do właściwych umów o współpracy,
- ewidencję upoważnień w rejestrze osób upoważnionych do przetwarzania danych osobowych.

VI UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

- Podmiot wdraża stosowanie wzorców umów powierzenia przetwarzania danych osobowych.
    - Wzorzec dla administratora stosuje się w przypadku powierzenia przetwarzania danych osobowych zewnętrznym podmiotom przetwarzającym.
    - Wzorzec dla podmiotu przetwarzającego stosuje się w przypadku, gdy Podmiot wykonuje czynności przetwarzania danych osobowych, powierzone przez ich zewnętrznych administratorów.
- Dopuszcza się stosowanie wzorców umów dostarczonych przez kontrahentów, pod warunkiem ich udokumentowanej akceptacji przez najwyższe kierownictwo lub osobę przez nie wyznaczoną.
- Zabrania się powierzania przetwarzania danych osobowych bez odpowiedniej umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego, zgodnego z art. 28 RODO.

Podmiot przechowuje szablony umów powierzenia i zawarte umowy powierzenia w załączeniu do niniejszej Polityki Ochrony Danych.

VII ANALIZA RYZYKA

- Podmiot wdraża zasadę analizowania ryzyka naruszenia praw lub wolności osób, których dane osobowe podlegają przetwarzaniu.
- Szacowanie ryzyka odbywać się będzie na warunkach ustanowionych w załączniku.
- Zabrania się wdrażania nowych czynności przetwarzania danych osobowych, wdrażania nowych zasobów służących do ich przetwarzania, a także zmian środków ochrony danych osobowych, bez uprzedniego wykonania analizy ryzyka lub jej aktualizacji.
- Podmiot zobowiązuje się do aktualizacji analizy ryzyka, znajdującej się w załączniku.

Podmiot przechowuje dokumentację szacowania ryzyka w załączeniu do niniejszej Polityki Ochrony Danych.

VIII OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

- Podmiot wdraża zasadę, aby monitorować czynności przetwarzania danych osobowych, w celu stwierdzenia, czy wymagają one wykonania OSOD-u (oceny skutków dla ochrony danych osobowych).
- W przypadku gdy dana czynność wymaga przeprowadzenia OSOD-u, stosuje się szablon znajdujący się w załączniku.
- Zabrania się wdrażania nowych czynności przetwarzania danych osobowych bez uprzedniego wykonania analizy ryzyka lub jej aktualizacji, a w przypadku gdy potwierdzi ona takową zasadność, bez przeprowadzenia OSOD-u.

Podmiot przechowuje szablon oceny skutków dla ochrony danych osobowych oraz dokumentację wykonanych ocen w załączeniu do niniejszej Polityki Ochrony Danych.

IX ŚRODKI OCHRONY DANYCH OSOBOWYCH

Uwzględniając zalecenia z przeprowadzonej analizy ryzyka oraz wymogi ustanowione w art. 32 RODO:

- Podmiot wdraża środki ochrony danych osobowych wymienione w załączniku – Rejestrze środków ochrony danych. Zabrania się wdrażania zmian środków ochrony danych osobowych, bez ich zewidencjonowania. Ponadto zobowiązuje się do ich aktualizacji.
- Podmiot wdraża procedury (organizacyjne środki ochrony danych osobowych), wymienione w załączniku – Procedury. Zabrania się wdrażania zmian wdrożonych procedur, bez ich uchwalenia zgodnie z zasadami reprezentacji. Ponadto zobowiązuje się do ich aktualizacji.
- Podmiot wdraża rejestr urządzeń oraz rejestr aplikacji, służących do przetwarzania danych osobowych. Zabrania się wdrażania urządzeń lub aplikacji niezewidencjonowanych w wymienionych rejestrach. Ponadto zobowiązuje się do ich aktualizacji.

Podmiot przechowuje wymienioną dokumentację w załączeniu do niniejszej Polityki Ochrony Danych.

X MIERZENIE I TESTOWANIE

Podmiot zobowiązuje się do regularnego testowania, mierzenia i oceniania skuteczności środków ochrony danych osobowych, w szczególności poprzez:

- bieżącą aktualizację rejestru naruszeń ochrony danych osobowych, analizy ryzyka, rejestru środków ochrony danych osobowych i wdrożonych procedur, rejestrów urządzeń i aplikacji, rejestru przeglądów i konserwacji systemu IT, a także rejestru istotnych czynności w systemie IT.
- wykonywanie audytów systemu przetwarzania danych osobowych,
- ewidencjonowanie audytów systemu przetwarzania danych osobowych w rejestrze audytów systemu przetwarzania danych osobowych.

Podmiot przechowuje rejestr audytów systemu przetwarzania danych osobowych w załączeniu do niniejszej Polityki Ochrony Danych.

XI INSPEKTOR OCHRONY DANYCH

- **Podmiot powołał Inspektora Ochrony Danych**, zgodnie z dokumentem znajdującym się w załączniku do niniejszej Polityki Ochrony Danych.

XII MONITORING

Podmiot nie stosuje żadnych form monitoringu.

XIII ZAŁĄCZNIKI

Załączniki do niniejszej Polityki Ochrony Danych stanowią jej integralną część:

A - LISTA ZAŁĄCZNIKÓW A (dokumenty podstawowe):

1. Rejestr czynności przetwarzania danych osobowych,
2. Rejestr kategorii czynności przetwarzania danych osobowych,
3. Rejestr naruszeń ochrony danych osobowych,
4. Rejestr środków ochrony danych osobowych,
5. Rejestr odbiorców danych osobowych,
6. Obowiązki informacyjne,
7. Upoważnienie dla pracowników - szablon,
8. Upoważnienie dla osób zatrudnionych na podstawie umów cywilnoprawnych - szablon,
9. Umowa powierzenia przetwarzania danych osobowych dla administratora - szablon,
10. Umowa powierzenia przetwarzania danych osobowych dla podmiotu przetwarzającego – szablon,
11. Analiza ryzyka – dokument przewodni,
12. Matryce ryzyk,
13. Ocena skutków dla ochrony danych - szablon,
14. Oświadczenie o powołaniu Inspektora Ochrony Danych,

B - LISTA ZAŁĄCZNIKÓW B (procedury – organizacyjne środki ochrony danych):

1. Procedura postępowania w przypadku naruszenia ochrony danych osobowych,
2. Procedura privacy by default,
3. Procedura ewidencjonowania urządzeń i nośników informacji,
4. Procedura korzystania z internetu,
5. Procedura korzystania z komputera służbowego,
6. Procedura korzystania z telefonu służbowego,
7. Procedura korzystania z poczty elektronicznej,
8. Procedura korzystania z urządzeń przenośnych,
9. Procedura postępowania z hasłami i plikami dostępowymi,
10. Procedura powierzenia przetwarzania danych osobowych,
11. Procedura privacy by design,
12. Procedura przeglądów i konserwacji systemu informatycznego,
13. Procedura przetwarzania danych osobowych w formie papierowej,
14. Procedura przyjmowania danych osobowych w powierzenie,
15. Procedura realizacji obowiązku informacyjnego,
16. Procedura usuwania danych osobowych,
17. Procedura realizacji żądań podmiotu danych,
18. Procedura tworzenia kopii zapasowych,
19. Procedura udostępniania danych osobowych,

20. Procedura dostępu do kluczy i obiektów,
21. Procedura usuwania urządzeń i nośników informacji,
22. Procedura kontroli dostępu do systemu informatycznego,
23. Procedura zabezpieczenia antywirusowego,

C - LISTA ZAŁĄCZNIKÓW C (dokumenty dodatkowe):

1. Rejestr osób upoważnionych do przetwarzania danych osobowych,
2. Rejestr audytów systemu przetwarzania danych osobowych,
3. Rejestr urządzeń służących do przetwarzania danych osobowych,
4. Rejestr aplikacji służących do przetwarzania danych osobowych,
5. Rejestr przeglądów i konserwacji systemu informatycznego,
6. Rejestr istotnych czynności w systemie informatycznym.

Podpis Administratora	Data