POLITIKA GDPR

Politika ochrany osobních údajů a systému řízení bezpečnosti informací společnosti

Vedení společnosti vyhlašuje následující Bezpečnostní politiku v souladu s řízením bezpečnostních incidentů a v souladu s Nařízením o ochraně osobních údajů.

Definice strategie informační bezpečnosti

Informační bezpečnost je chápána jako celek složený z jednotlivých opatření organizační bezpečnosti, zajištění ochrany osobních údajů, personální a fyzické bezpečnosti a bezpečnosti informačních technologií pro zajištění dostupnosti, integrity a důvěrnosti informací organizace.

Bezpečnostní opatření - kritéria hodnocení rizik

Bezpečnostní opatření jsou vybrána na základě prováděného hodnocení rizik a požadavků zákonných a jiných norem.
Hodnocení rizik má za cíl určit možné hrozby, zranitelnosti a rizika hodnoceného systému, odhadnout ztráty, které mohou vzniknout působením hrozeb při správě osobních údajů organizací. Hodnocení rizik se provádí s využitím analýzy rizik. Postup provádění analýzy rizik je podrobně popsán v Příloze č. 3 Analýza a vyhodnocení a rizik pro práva a svobody fyzických osob, Příručky GDPR.
Analýza rizik je aktualizována jedenkrát za rok, nebo v případě změn v informačních systémech a změn v požadavcích na informační a kybernetickou bezpečnost.

Politika řízení bezpečnostních incidentů (porušení zabezpečení osobních údajů)

Bezpečnostní incident tvoří jedna nebo série nežádoucích neočekávaných událostí informační bezpečnosti, které mají podstatnou šanci ohrozit informační bezpečnost organizace.
Cílem správy bezpečnostních incidentů je zabránit přerušení nebo poškození činností organizace, nebo poškození dobrého jména organizace, umožnit včasnou nápravu s využitím formalizovaného a obecně známého postupu.
Pro zajištění zpětné vazby při řešení bezpečnostních incidentů je prováděno jejich vyhodnocení. Vyhodnocení se využívá pro zpracování dodatečných nebo důkladnějších opatření, která by snižovala pravděpodobnost, závažnost a dopad budoucích výskytů bezpečnostních incidentů.

Registr bezpečnostních incidentů

Správa bezpečnostních incidentů je vedena v Registru událostí a incidentů, příloha č. 1 této Bezpečnostní politiky.

Postupy pro identifikaci a reakci na bezpečnostní incidenty

Organizace vede záznamy všech bezpečnostních incidentů (případů porušení zabezpečení osobních údajů) a některá porušení oznámí Úřadu pro ochranu osobních údajů.
V případě výskytu incidentu, bude tento incident zaznamenán. Záznam musí obsahovat:

- **Popis případu**
- **Účinky porušení zabezpečení**
- **Přijetí opatření**
- **Oznámeno**

Oznámení porušení zabezpečení ÚOOÚ

Úřadu pro ochranu osobních údajů je třeba oznamovat jen takové případy, které představují reálné riziko pro práva a svobody fyzických osob. K posouzení, zda porušení zabezpečení je rizikové, je možné vycházet z hodnot dopadů konkrétní realizované hrozby na konkrétní právo

subjektu údajů daného záznamu (viz systém GDPR/ Hrozby a rizika pro práva a svobod fyzických osob), kdy stupně 3, 4 a 5 jsou doporučeny ÚOOÚ oznamovat.

Závažnosti dopadu konkrétní realizované hrozby na konkrétní právo subjektu údajů		
stupeň	*textové vyjádření stupně dopadu*	*bližší popis*
1	nevýznamný	dopad na konkrétní právo SU je pro SU nevýznamný, SU si následek dopadu vůbec neuvědomí
2	přijatelný	dopad na konkrétní právo SU je pro SU přijatelný, SU si následek dopadu uvědomuje, ale nepocítí žádnou změnu ve svém životě, a nebude muset na nastalou situaci nijak reagovat
3	citelný	dopad na konkrétní právo SU je pro SU citelný, SU si následek dopadu uvědomuje, následek může vyvolat u SU pocit diskomfortu v jeho životě, ale nebude muset na nastalou sizuaci nijak reagovat
4	vážný	dopad na konkrétní právo SU je pro SU vážný, SU si následek dopadu uvědomuje, následek vyvolá u SU diskomfort v jeho životě, a SU bude muset vyvinout činnost k nápravě stavu
5	velmi vážný	dopad na konkrétní právo SU je pro SU velmi vážný, SU si následek dopadu uvědomuje, následek může vyvolat u SU omezení jeho práv, a SU bude muset vyvinout náročnou činnost k nápravě stavu

Pověřený zástupce organizace **vždy** přezkoumá míru porušení zabezpečení osobních údajů a na základě přezkoumání rozhodne o odeslání/neodeslání Oznámení.

Obsah a lhůta pro oznámení

Obsahové náležitosti oznámení jsou přílohou č. 2 této Bezpečnostní politiky. Oznámení musí být učiněno do 72 hodin od zjištění bezpečnostního incidentu. V případě pozdějšího oznámení je nutné zpoždění zdůvodnit.

Oznámení porušení zabezpečení subjektům údajů

Subjektům údajů je třeba oznamovat jen takové případy, které pravděpodobně způsobí vysoká rizika pro práva a svobody fyzických osob. K posouzení, zda porušení zabezpečení je **vysoce rizikové**, je možné vycházet z hodnot dopadů konkrétní realizované hrozby na konkrétní právo subjektu údajů daného záznamu (viz systém GDPR/ Hrozby a rizika pro práva a svobod fyzických osob). Kdy stupně 4 a 5 jsou doporučeny SÚ oznamovat.

Závažnosti dopadu konkrétní realizované hrozby na konkrétní právo subjektu údajů		
stupeň	*textové vyjádření stupně dopadu*	*bližší popis*
1	nevýznamný	dopad na konkrétní právo SU je pro SU nevýznamný, SU si následek dopadu vůbec neuvědomí
2	přijatelný	dopad na konkrétní právo SU je pro SU přijatelný, SU si následek dopadu uvědomuje, ale nepocítí žádnou změnu ve svém životě, a nebude muset na nastalou situaci nijak reagovat
3	citelný	dopad na konkrétní právo SU je pro SU citelný, SU si následek dopadu uvědomuje, následek může vyvolat u SU pocit diskomfortu v jeho životě, ale nebude muset na nastalou sizuaci nijak reagovat
4	vážný	dopad na konkrétní právo SU je pro SU vážný, SU si následek dopadu uvědomuje, následek vyvolá u SU diskomfort v jeho životě, a SU bude muset vyvinout činnost k nápravě stavu
5	velmi vážný	dopad na konkrétní právo SU je pro SU velmi vážný, SU si následek dopadu uvědomuje, následek může vyvolat u SU omezení jeho práv, a SU bude muset vyvinout náročnou činnost k nápravě stavu

Pověřený zástupce organizace **vždy** přezkoumá míru porušení zabezpečení osobních údajů a na základě přezkoumání rozhodne o odeslání/neodeslání Oznámení.

Obsah a lhůta pro oznámení

Obsahové náležitosti oznámení jsou přílohou č. 3 této Bezpečnostní politiky. Oznámení musí být učiněno bez zbytečného odkladu.

Přílohy

Příloha č. 1 Registru bezpečnostních incidentů
Příloha č. 2 Oznámení porušení zabezpečení ÚOOÚ
Příloha č. 3 Oznámení porušení zabezpečení subjektům údajů

Příloha č. 1
Registr bezpečnostních incidentů
Legenda:

- **Popis případu** (To je v podstatě popis toho, k čemu došlo.)
- **Účinky porušení zabezpečení** (Zde je třeba stručně popsat, jaký dopad incident měl.)
- **Přijetí opatření** (Je třeba stručně uvést, co jste udělali pro to, aby k podobnému incidentu již nedošlo.)
- **Oznámeno** (Zapíšete poznámku, zda jste incident oznámili Úřadu pro ochranu osobních údajů a subjektům údajů (ANO), nebo neoznámili (NE) s krátkým zdůvodněním).

Stupnice hodnocení závažnosti:

Závažnosti dopadu konkrétní realizované hrozby na konkrétní právo subjektu údajů

stupeň	*textové vyjádření stupně dopadu*	*bližší popis*
1	nevýznamný	dopad na konkrétní právo SU je pro SU nevýznamný, SU si následek dopadu vůbec neuvědomí
2	přijatelný	dopad na konkrétní právo SU je pro SU přijatelný, SU si následek dopadu uvědomuje, ale nepocítí žádnou změnu ve svém životě, a nebude muset na nastalou situaci nijak reagovat
3	citelný	dopad na konkrétní právo SU je pro SU citelný, SU si následek dopadu uvědomuje, následek může vyvolat u SU pocit diskomfortu v jeho životě, ale nebude muset na nastalou sizuaci nijak reagovat
4	vážný	dopad na konkrétní právo SU je pro SU vážný, SU si následek dopadu uvědomuje, následek vyvolá u SU diskomfort v jeho životě, a SU bude muset vyvinout činnost k nápravě stavu
5	velmi vážný	dopad na konkrétní právo SU je pro SU velmi vážný, SU si následek dopadu uvědomuje, následek může vyvolat u SU omezení jeho práv, a SU bude muset vyvinout náročnou činnost k nápravě stavu

Datum zjištění	Popis případu	Účinky porušení zabezpečení	Závažnost	Oznámeno ÚOOÚ	Oznámeno SÚ

Příloha č. 2
Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7

Ohlášení porušení zabezpečení osobních údajů

I. Správce osobních údajů

Association Club Sparta Praha z.s. …… *(jméno a příjmení, nebo obchodní firma)*

43005802 *(identifikační číslo osoby – IČO)*

Kovanecká 2405/27, Praha 9 – Libeň *(sídlo)*

sokolovska@acspartapraha.cz *(elektronická adresa)*

II. Datum a popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů

III. Jméno a kontaktní údaje osoby, která může poskytnout bližší informace

IV. Popis pravděpodobných důsledků porušení zabezpečení osobních údajů

V. Popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů

V ……... dne ……. …….

podpis správce nebo osoby
zastupující správce

Příloha č. 3
Přímo SÚ
(pokud by oznámení přímo subjektům údajů vyžadovalo nepřiměřené úsilí, potom je zvolen jiný, stejně účinný způsob, např. veřejné oznámení apod.)

Ohlášení porušení zabezpečení osobních údajů

I. Správce osobních údajů

Association Club Sparta Praha z.s. …… *(jméno a příjmení, nebo obchodní firma)*

…… *(identifikační číslo osoby – IČO)*

…… *(sídlo)*

…… *(elektronická adresa)*

II. Datum daného případu porušení zabezpečení osobních údajů

III. Jméno a kontaktní údaje osoby, která může poskytnout bližší informace

IV. Popis pravděpodobných důsledků porušení zabezpečení osobních údajů

V. Popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů

V ……... dne ……. ……

podpis správce nebo osoby
zastupující správce