Technická a organizační zařízení dle GDPR

I. Zabezpečení zpracování (článek 32 odstavec 1 písmeno a + b GDPR)

1. Kontrola přístupu do oblastí zpracování (fyzický přístup)

- Existence fyzické bezpečnostní koncepce pro relevantní pracoviště, včetně fyzických bezpečnostních zón.
- Zajištění přiměřené kontroly přístupu do budov a oblastí, které se nacházejí v různých fyzických bezpečnostních zónách.
- Omezení fyzického přístupu na potřebné minimum (princip minimálního oprávnění).
- Zajištění fyzické ochrany perimetru, budov a prostor prostřednictvím oplocení, bezpečnostních dveří a oken.
- Správa klíčů a přístupových karet.
- Omezení přístupu do datových center na velmi výrazně omezenou skupinu autorizovaných osob, včetně opatření pro zjištění neoprávněného vniknutí.
- Správa návštěv na pracovištích.

2. Kontrola přístupu k systémům zpracovávajícím data (autentizace)

- Zajištění silné autentizace uživatelů (MFA) pro operativní personál, který na aplikaci pracuje.
- Autentizace technických uživatelů prostřednictvím zabezpečených autentizačních protokolů.
- Zajištění síťové autentizace mezi systémy nebo nebo systémových komponent prostřednictvím certifikátů zařízení (rozhraní).
- Autentizace jiných aplikací s použitím technických uživatelů prostřednictvím zabezpečených autentizačních protokolů.
- Zajištění dodržování principů „Clear-Screen“, „Clean-Desk“ a „Clean-Wall“ na pracovištích a prostřednictvím osob v oblasti platnosti služeb zpracovávající osobní údaje.
- Zajištění DMZ a Application Gateway pro přístup k externím sítím (např. na internet).
- Implementace ochrany před malwarem (včetně EDR na klientských počítačích a serverech).

3. **Kontrola přístupu k používání určitých oblastí systémů zpracování dat (autorizace)**
   - Dokumentace koncepce rolí a oprávnění.
   - Omezení přístupu na potřebné minimum (princip minimálního oprávnění).
   - Využití personalizovaných účtů uživatelů pro operativní personál, který na aplikaci pracuje.
   - Zabránění přístupu k aplikaci přes standardní nebo testovací účty.
   - Využití procesu pro pravidelnou kontrolu a pro odebrání oprávnění.
   - Vytvoření samostatných administrátorských účtů pro správu systémů.
   - Zajištění bezpečného smazání a likvidace (jak dat, tak fyzických dokumentů), pokud již nejsou potřeba.
   - Zajištění, že aplikace poskytují multitenantní architekturu nebo dedikované systémy pro zpracování dat pro různé účely.
4. **Oddělení zpracování pro různé účely**
   - Používání různých prostředí pro vývoj, testování/zajištění kvality a výrobu.
5. **Pseudonymizace**
   - Zajištění, že budou před použitím dat pro jiný účel, než pro který byla původně získána, z datových záznamů odstraněna (anonymizována) data odkazující na konkrétní osobu.
6. **Šifrování**
   - Používání šifrování dle aktuálního stavu techniky (state-of-the-art) pro zabezpečení dat v klidu (Data at Rest).

II. Integrita (článek 32 odstavec 1 písmeno b GDPR)

1. **Kontrola zadávání**
   - Zaznamenávání přihlášení uživatelů a nepodařených pokusů o přihlášení.
   - Protokolování akcí správy uživatelů.
   - Stanovení lhůt pro ukládání a mazání dat protokolů.
   - Zajištění validace zadávání.
2. **Kontrola přenosu**
   - Koordinování dohod rozhraní.
   - Používání Transport Layer Security (autentizace a šifrování) pro zpracování dat dle stavu techniky (state-of the-art).

- Oddělení přímého externího přístupu k aplikaci.
- Protokolování příchozí a odchozí datové komunikace.
- Zajištění kódování pro příslušný cílový systém výstupních dat.

III. Dostupnost a odolnost (článek 32 odstavec 1 písmeno b GDPR)

1. Kontrola dostupnosti

- Implementace ochrany před malwarem (včetně EDR na klientských počítačích a serverech).
- Pravidelné získávání/vyžádávání informací o slabých místech softwaru.
- Odstraňování slabých míst dle definovaných dob odstranění, v závislosti na kritičnosti.
- Pravidelná identifikace a odstraňování nedostatků.
- Implementace zálohování dle koncepce zálohování.
- Zajištění, že bude pravidelně prováděn test obnovení záloh.
- Provádění pravidelných bezpečnostních kontrol pro vyhledávání slabých míst a nedostatků během vývoje (statická a dynamická bezpečnostní analýza).
- Provádění pravidelných bezpečnostních analýz pro vyhledávání slabých míst a nestandardního chování pro větší nová vydání nebo větší změny funkcí (penetrační testy).
- Odstraňování identifikovaných slabých míst a nestandardního chování v závislosti na jejich kritičnosti.
- Poskytnutí cold-standby systému.
- Zajištění přiměřených fyzických opatření pro obchodní kontinuitu pro výpočetní centra a jinou relevantní IT infrastrukturu (včetně redundantního napájení elektrickým proudem, síťových propojení, ochrany vody, hasicího zařízení).
- Provoz centrální organizace pro management slabých míst pro všechny dotčené systémy.

IV. Proces pravidelného testování, posuzování, hodnocení a evaluace účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování dat (článek 32 odstavec 1 písmeno d GDPR)

1. Management ochrany dat

- Potvrzení potřeby ochrany klasifikace bezpečnosti informací pro (zúčastněné informační hodnoty).
- Pravidelná kontrola dodržování požadavků na službu.
- Zohlednění bezpečnostních standardů při vývoji aplikace (Security by Design)
- Zohlednění požadavků na ochranu dat při vývoji aplikace (Privacy by Design)
- Zajištění dodržování požadavků compliance a pravidel při používání open source softwaru.
- Plánování a dokumentace životního cyklu softwaru aplikace.
- Zvýšení citlivosti administrátorů aplikace na IT bezpečnost.
- Provoz systému řízení bezpečnosti informací (ISMS) s dedikovanými rolemi bezpečnosti informací, které jsou zodpovědné za zajištění implementace přiměřených opatření pro zajištění bezpečnosti informací, pravidelné hodnocení jejich účinnosti a v případě potřeby úprava opatření.
- Provoz systému řízení ochrany dat (DPMS) s dedikovanými rolemi ochrany dat, které jsou zodpovědné za dokumentaci činností zpracování, implementaci přiměřených opatření ochrany dat, pravidelné hodnocení jejich účinnosti a v případě potřeby úprava opatření.

2. Incident-Response-Management

- Definice událostí ohrožujících bezpečnost informací ve vztahu k aktivitám uživatele.
- Používání synchronizovaného časového razítka při protokolování aktivit uživatele.
- Pravidelná analýza protokolových dat pro kontrolu, zda se vyskytly události nebo případy ohrožující bezpečnost informací.
- Provoz nepřetržité služby Incodent-Response, která zajistí, že budou události ohrožující bezpečnost informací co nejdříve analyzovány a bude se na ně reagovat.
- Udržování reakčních plánů pro relevantní případy ohrožení bezpečnosti informací.

3. **Ochrana dat prostřednictvím přednastavení vhodných pro ochranu dat (článek 25 odstavec 2 GDPR)**

   - Zajištění, že při získávání a používání osobních údajů budou jako povinné označeny jen osobní údaje, které jsou potřeba k určitému účelu.

4. **Kontrola zpracování**

   - Zajištění, že subdodavatelé budou pečlivě vybíráni, budou s nimi uzavřeny smlouvy o zpracování a technická a organizační opatření budou předána také na zpracování subdodávek..
   - Zajištění, že všechny osobní údaje použité v rámci zpracování budou na konci servisní smlouvy smazány, s výjimkou případu, kdy existuje zákonná povinnost jejich delšího uchovávání.
   - Zajištění pravidelných školení k bezpečnosti informací, včetně akceptovatelného používání při práci s informacemi, pro všechny zaměstnance, kteří mají přístup k datům aplikace.
   - Zajištění, že budou všichni zaměstnanci, kteří mají přístup k osobním údajům, zavázán k zachovávání důvěrnosti.