XLAB s.r.o.

POLITIKA BEZPEČNOSTI INFORMACÍ A OSOBNÍCH ÚDAJŮ

Společnost XLAB s.r.o., se sídlem Výstaviště 67, 170 00 Praha 7, ČR (dále jen „ **Xlab**“) podporuje budování a neustálé rozvíjení systému řízení bezpečnosti informací, aby tím chránila aktiva a aby svým pracovníkům, zákazníkům i partnerům poskytla odpovídající míru jistoty.

Z tohoto důvodu vedení XLAB schvaluje a vyhlašuje tuto politiku bezpečnosti informací a osobních údajů XLAB jako rámec pro směřování společnosti na poli ochrany bezpečnosti informací. Záměrem vedení je podporovat vytyčené cíle a principy této politiky.

Stanovená politika bezpečnosti je přiměřená záměrům XLAB, a zahrnuje cíle bezpečnosti informací k osobním údajům, a to s přihlédnutím k základním koncepčním požadavkům kladeným zejména v mezinárodně uznávané normě ISO/IEC 27002 a na ní navazující normy ISO/IEC 2700X. Tyto mezinárodně uznávané směrnice definují požadavky na systém managementu bezpečnosti informací.

Politika bezpečnosti informací k osobním údajům, komunikována v rámci celé organizační struktury, je dostupná jako dokumentovaná informace a přiměřeně dostupná zainteresovaným třetím stranám.

Touto politikou XLAB deklaruje všem obchodním partnerům, pracovníkům, veřejné a státní správě a široké veřejnosti schopnost efektivně chránit informace, hmotný i nehmotný majetek vlastní i svěřený v souladu s legislativními požadavky s platnou legislativou České republiky i Evropské unie, mezinárodními smlouvami a jinými požadavky na ochranu bezpečnosti informací.

Pro účely této politiky bezpečnosti informací XLAB se definují **:**

- **„aktiva“** jsou osobní údaje XLAB;
- **„XLAB“** je společnost XLAB s.r.o., se sídlem Výstaviště 67, 170 00 Praha 7, ČR; zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl C, vložka 213941;
- **„incident“** znamená zjištěný výskyt stavu systému, stavu služby nebo stavu sítě naznačující možné narušení politiky bezpečnosti informací nebo selhání opatření a další;
- **„občanský zákoník“ nebo „OZ“** znamená zákon č. 89/2012 Sb., občanský zákoník;
- **„osobní údaje“** jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
- **„osoba pověřená zpracováním“** znamená osoba pověřená XLAB, která na základě pracovní smlouvy, smlouvy o poskytování služeb, dohod uzavřených mimo pracovní poměr anebo dalších smluv či dohod uzavřených s Xlab při výkonu své funkce zpracovává nebo má přístup k osobním údajům;

- **„osoba s oprávněním“** je osoba pověřená zpracováním osobních údajů XLAB se zvláštním přístupem definovaným uživatelským jménem/označením, a to na základě pokynu, plnění smlouvy či jiné skutečnosti, které bylo přiděleno uživatelské jméno/označení, na základě kterého jí je umožněn zvláštní přístup k osobním údajům;

- **„platformy XLAB“** jsou veškeré platformy, které společnost XLAB spravuje, vlastní, řídí, vyvíjí nebo se na jejich chodu zásadním způsobem podílí, včetně platformy XLAB, která slouží k organizování společenských, sportovních, kulturních či jiných událostí;

- **„politika bezpečnosti“** znamená tuto politiku bezpečnosti informací XLAB k osobním údajům;

- **„úložiště“,** popř. server je centrální místo kde dochází k ukládání dat a jejich udržování;

- **„zákoník práce“** nebo **„ZP“** znamená zákon č. 262/2006 Sb., zákoník práce;

- " **zpracovatel údajů** ", " **správce údajů** ", **„osobní údaj“** a " **zpracování** " mají stejný význam, jaký jim připisuje **GDPR** .

- Ostatní pojmy v této smlouvě obsažené mají stejný význam, jaký jim připisuje norma **ISO/IEC 27000.**

Vymezení aktiv XLAB
Aktiva XLAB, tvoří veškeré osobní údaje týkající se pracovníků XLAB, osobní údaje obchodních partnerů XLAB, osobní údaje získané od zákazníků v rámci poskytování služeb ze strany Xlab a uživatelů platforem XLAB**.** XLAB je oprávněn na základě smluvních vztahů s pracovníky, zákazníky a obchodními partnery mít přístup k jejich osobním údajům a zpracovávat je, a to v souladu s vysokými standardy ochrany osobních údajů, jejichž průmětem je, mj. tato Politika bezpečnosti.

XLAB zpracovává osobní údaje zejména při následujících činnostech:

- Provozování platforem XLAB
- Monitoring zákazníků a uživatelů platforem XLAB prostřednictvím logů
- Při poskytování služeb zákazníkům a obchodním parterům XLAB
- Při přípravě a realizaci eventů
- Archivace smluvní dokumentace

Politika bezpečnosti osobních údajů XLAB je vymezena v následujících bodech tohoto dokumentu. Jednotlivé body obsahují informace týkající se organizačně-bezpečnostních opatření, přidělených funkcí/rolí a s nimi spojené odpovědnosti, řízení kontroly přístupu k systémům a aplikacím, řízení aktiv a zabezpečení mlčenlivosti pracovníků a dalších osob a dalších.

1. Organizační a bezpečnostní opatření

Osobní údaje by měly být zpracovávány způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a k zařízení používanému k jejich zpracování nebo jejich neoprávněnému použití. XLAB dohlíží na to, aby osobní údaje subjektů údajů byly zpracovány korektně a zákonným a transparentním způsobem. Dále dohlíží, aby osobní údaje subjektů údajů byly shromažďovány pro určité, výslovně vyjádřené a legitimní účely a aby nedocházelo k jejich zpracování způsobem, který je s těmito účely neslučitelný.

XLAB při zpracování osobních údajů subjektů údajů dbá na to, aby osobní údaje byly přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovány.

XLAB si je vědom, že zpracovávané osobní údaje subjektů údajů musí být přesné a v případě potřeby aktualizované, musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny, dále že osobní údaje musí být uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány.

XLAB přijímá s ohledem na povahu, rozsah a účely zpracování technická a organizační opatření, aby zajistila soulad zpracování osobních údajů s Nařízením.

a) Bezpečnost lidských zdrojů

Osoby pověřené zpracováním jsou srozuměny se svými povinnostmi. Při výběru pracovníka do XLAB je každý uchazeč prověřen podle platných právních předpisů, tj. zejména zákoník práce, občanský zákoník a v souladu s etikou.

Přijímání pracovníků je s přihlédnutím k obvyklé praxi XLAB interní postup, jehož výsledkem je, za splnění přísných kritérií a s ohledem na vysoký standard požadovaný po všech pracovnících, výběr toho nejvhodnějšího uchazeče. Každý uchazeč je tak před zahájením výkonu práce:

- *seznámen s vnitropodnikovými postupy a doporučeními XLAB. Každá osoba pověřená zpracováním je povinna dodržovat tyto postupy a doporučení zavedené v rámci celé XLAB, a to v souladu s touto politikou bezpečnosti*

Během zpracovávání osobních údajů XLAB má osoba takto pověřená povinnost
zejména:

- *veškeré informace a data uchovávat na firemním serveru/úložišti;*

- *k přenosu těchto dat využívat pouze přidělené pracovní pomůcky;*

- *nestahovat data ze serveru/úložiště na jiná pevná úložiště, pokud není se zákazníkem dohodnuto jinak, taková dohoda pak musí být potvrzena písemně, minimálně v emailové komunikaci;*

- *neuchovávat data mimo firemní server/úložiště, pokud není se zákazníkem dohodnuto jinak, taková dohoda pak musí být potvrzena písemně, minimálně v emailové komunikaci;*

V případě změny pracovní pozice, náplně práce či obsahu funkce přidělené osobě pověřené zpracováním, bude aktualizován rozsah přístupu k osobním údajům takové pověřené osoby. Každá osoba pověřená zpracováním, u které došlo k takové skutečnosti, má povinnost zejména:

- *neprodleně svého nadřízeného informovat, pokud zjistí, že došlo k nesprávné formě aktualizace přístupu k osobním údajům;*

- *tato data aktivně nevyhledávat, nestahovat, dále nijak nepoužívat, s nimi nijak nenakládat, či zveřejňovat;*

- *neprodleně svého nadřízeného informovat, pokud zjistí, že má jiný přístup k datům;*

Každé osobě pověřené zpracováním bude po rozvázání pracovního poměru, ukončení smlouvy o poskytování služeb či jiného obdobného způsobu ukončení spolupráce se XLAB znemožněn přístup k osobním údajům XLAB. Osoba pověřená zpracováním před ukončením smluvního závazku se XLAB zejména:

- *neprodleně firmě XLAB oznámí, pokud zjistí, že má i nadále jakýkoliv přístup k datům*

- *na základě výstupního formuláře odevzdá přidělené pracovní pomůcky*

Co se stane s přístupy osoby v případě rozvázaní pracovního poměr/ukončení poskytování služeb:

- *v den rozvázání pracovního, popř. obdobného smluvního vztahu je osobě s oprávněním zrušen účet*

- *samotným zrušením účtu tato osoba automaticky ztrácí přístup do všech dalších toolů, jelikož jsou na tento uživatelský účet navázány*

V případě, že osoba pověřená zpracováním poruší povinnosti stanovené v rámci celé XLAB, zejména v této politice bezpečnosti, jakožto i další povinnosti uložené prostřednictvím pokynů, příkazů a doporučení ze strany XLAB, je vytvořena klasifikace základních přestupků a k nim přiřazené příslušné sankce.

- *v případě malého pochybení v rámci bezpečnosti informací bude uložena dotyčné osobě výtka*

- *v případě středního pochybení v rámci bezpečnosti informací bude dotyčná osoba povinna podstoupit konfrontaci s vedením* XLAB *a tato osoba bude nově proškolena*

- *v případě hrubého pochybení v rámci bezpečnosti informací bude s dotyčnou osobou rozvázán pracovní, popř. obdobný vztah*

b) Fyzická bezpečnost a bezpečnost prostředí

XLAB dbá při zpracování svých aktiv na zajištění bezpečnosti prostoru a prostředí, kde dochází ke zpracování osobních údajů. Každá osoba pověřená zpracováním dbá postupů a mechanismů stanovených XLAB.

Fyzická bezpečnost kanceláří pracovníků je zajištěna prostřednictvím uzamykatelných dveří takových kanceláří, přičemž přístup do nich mají pouze oprávněné osoby.

XLAB dbá zásady tzv. prázdného stolu a prázdné obrazovky monitoru. Těmito zásadami se má na mysli zejména to, aby se osobní údaje zaznamenané v listinné podobě nenacházely volně v prostorách kanceláří, ale aby tyto listinné dokumenty byly bezpečně uloženy v prostorách se zabezpečeným a omezeným přístupem.

Dále XLAB dbá na to, aby počítače a jiné terminály byly ponechávány s odhlášenými osobami s oprávněním nebo chráněny mechanismem zamykajícím obrazovku nebo klávesnici.

Zařízení XLAB, která zpracovávají (ukládají) osobní údaje XLAB jsou umístěna a chráněna tak, aby došlo ke snížení rizika hrozeb a nebezpečí. XLAB má zavedené postupy pro bezpečnou likvidaci zařízení, včetně odstranění osobních údajů na nich uložených.

c) Správa bezpečnosti sítě

XLAB prostřednictvím pověřených osob zajišťuje ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací, zároveň si je vědoma potřeby oddělení skupiny informačních služeb, osob s oprávněním a informačních systémů v jednotlivých sítích.

Ve firmě jsou také zavedeny bezpečnostní mechanismy používaných síťových služeb, provozní postupy a opatření pro ochranu informací proti malwaru, postupy pro zálohování informací, postupy řízené instalace a pravidelné aktualizace softwarů na provozních systémech včetně zavedení šifrování komunikace pomocí bezpečnostního HTTPS certifikátu.

XLAB dbá na zajištění maximální bezpečnosti informací také skrze komunitu OWASP, ke kterému se hlásí. OWASP je komunita zabývající se bezpečností webových aplikací.

d) Přenos informací

XLAB dbá na bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty. Ochrana se vztahuje na aktiva přenesená elektronicky i fyzicky.

Osoby pověřené zpracováním, mimo rozsah pravomocí jím svěřených v rámci přidělené funkce/role, nesmí bez souhlasu osoby odpovědné za dodržování politiky bezpečnosti, jakkoliv nakládat a manipulovat s osobními údaji XLAB.

e) Bezpečnostní incidenty

Jeden z požadavků dle čl. 5 odst. 1 písm. f) Nařízení je, aby při použití patřičných technických a organizačních opatření byly osobní údaje zpracovány způsobem zajišťujícím náležité zabezpečení včetně ochrany před neoprávněným nebo protiprávním zpracováním a náhodnou ztrátou, zničením nebo poškozením.

Pojem „zničení“ je dle Nařízení vykládáno jako případ, kdy údaje už neexistují vůbec nebo přinejmenším ne v podobě, aby byly k užitku.

Pojem „poškození“ je vykládán jako případ, kdy osobní údaje jsou pozměněna nebo už nejsou úplná.

„Ztráta“ osobních údajů je vykládána tak, že data sice mohou stále existovat, avšak XLAB nad nimi ztratil kontrolu nebo přístup k nim, či je už nemá v držení.

Neoprávněné nebo protiprávní zpracování dle Nařízení zahrnuje zpřístupnění osobních údajů příjemcům (nebo jejich přístup), kteří nemají oprávnění data získat (nebo mít k nim přístup) nebo jakoukoli jinou formu zpracování, která je v rozporu s Nařízením.

Z tohoto důvodu dbá XLAB, aby jako správce disponoval náležitými technickými a organizačními opatřeními pro zajištění takové úrovně zabezpečení, která odpovídá riziku, jež dané zpracování osobních údajů doprovází.

Dále XLAB bere v úvahu současný stav vývoje, náklady zavedení a povahu, rozsah, souvislosti a účely zpracování, stejně jako riziko proměnlivé pravděpodobnosti a závažnost pro práva a svobody fyzických osob.

XLAB si je vědom výše zmíněného požadavku, a to včetně požadavku, aby porušení zabezpečení osobních údajů bylo nahlášeno příslušnému národnímu dozorovému úřadu a v jistých případech došlo

ke sdělení informací o porušení zabezpečení osobních údajů jednotlivcům, jejichž osobní údaje byly tímto dotčeny.

Proto XLAB s předstihem plánuje a zavádí postupy umožňující odhalit a bezodkladně zvládnout případ porušení, posoudit riziko pro jednotlivce a pak určit, zda je nutné vyrozumět příslušný dozorový úřad a případně i dotčené jednotlivce.

Jako pomocné vodítko při řešení bezpečnostních incidentů využívá XLAB Vodítko k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679 (dále jen „Stanovisko“) jež vypracovala pracovní skupina WP29.

Na základě tohoto Stanoviska dochází k zařazení jednotlivých porušení do tří základních kategorií:

- „Porušení důvěrnosti“ – v případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů.
- „Porušení dostupnosti“ – v případě náhodné nebo neoprávněné ztráty přístupu nebo zničení osobních údajů.
- „Porušení integrity“ – v případě neoprávněného nebo náhodného pozměnění osobních údajů.

2. Pravidla řízení přístupu

Účelem řízení přístupu k informacím a prostředkům informačních systémů XLAB je zajistit, aby k nim měli přístup pouze osoby s oprávněním. Pro přístup k těmto prostředkům jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv.

Přístup do systému je povolen přihlášeným osobám s oprávněním podle přidělených oprávnění. U vytvořeného hesla jsou zadány požadavky na složitost – minimální délka hesla.

XLAB využívá v souladu s politikou bezpečnosti při zpracování osobních údajů standardní postupy, na základě kterých dochází k definování práv přístupu pro všechny pozice, přičemž pravidelně dochází k přezkoumávání přístupových práv jednotlivých osob s oprávněním. Přístupy osob s oprávněním jsou řízeny samostatně pouze k osobním údajům, které potřebuje k výkonu své činnosti.

Dále jsou zavedeny postupy pro odebírání nebo úpravu přístupových práv osob s oprávněním při ukončení nebo změně pracovního, popř. obdobného vztahu.

Přístup k aplikaci pro zákazníky je vždy povolen na základě vygenerovaného jména a hesla, které si zákazník může změnit a musí splňovat základní bezpečnostní nastavení – minimální délka.

Veškeré osobní údaje, které zákazník vloží do aplikace jsou uloženy v databázi na serveru provozovatele cloudových služeb. K těmto údajům má přístup pouze pověřená osoba.

a) Využívání jiných platforem k ukládání osobních údajů

Osobní údaje XLAB jsou dále ukládány primárně na virtuálních serverech, dále virtuální servery pro mail server a v rámci šíření interních dokumentů XLAB využívá Microsoft Sharepoint.

Přístup k těmto osobním údajům ukládaných na jiných platformách mají pouze osoby s oprávněním prostřednictvím účtu zabezpečeného vygenerovaným heslem.

Všichni provozovatelé virtuálních serverů, se kterými XLAB spolupracuje, byli vybráni na základě prostudování a vyhodnocení jejich technických a bezpečnostních opatřeních, kterými se reprezentují na svých webových stránkách, a dále na základě předchozích zkušeností s těmito provozovateli. (Např. implementace a soulad s požadavky kladenými mezinárodně uznávanou normou ISO/IEC 27018.)

3. Řízení aktiv

XLAB si je vědom všech oblastí v rámci kterých dochází ke zpracování osobních údajů a dokáže identifikovat vždy zdroj, od kterého osobní údaj získala a konkrétního vlastníka daného osobního údaje.

XLAB dbá na to, aby veškeré osobní údaje byly uchovány po dobu nezbytně nutnou k naplnění účelu, pro který byl osobní údaj získán a zároveň, aby splňovala zákonem uložené povinnosti týkající se doby uchování osobních údajů v evidenci. Osobní údaje zákazníků jsou po 5 letech nečinnosti anonymizovány.

Každý pracovník XLAB je dostatečně proškolen ohledně celkového řízení aktiv XLAB a je si vědom následků porušení povinnosti na něj v této souvislosti kladené.

XLAB v rámci bezpečnosti informací šifruje osobní údaje se kterými osoby pověřené zpracováním pracují. Dále veškeré dokumenty obsahující osobní údaje, které XLAB nemá ze zákona povinnost uchovávat, skartuje.

4. Dodržení standardů ochrany osobami pověřenými zpracováním

Každá osoba pověřená zpracováním dbá na dodržování vysokých standardů ochrany osobních údajů, se kterými byla seznámena, a vynaloží maximální úsilí, aby nedošlo k neoprávněnému zpracování osobních údajů.

Mezi každou osobou pověřenou zpracováním a XLAB byl vytvořen smluvní vztah, a to na základě pracovní smlouvy, smlouvy o poskytování služeb, dohody uzavřené mimo pracovní poměr nebo další obdobné smlouvy či dohody.

K dodržení vysokého standardu ochrany osobních údajů obsahují jednotlivé smlouvy a dohody ochranné doložky včetně dílčích povinností, tj. například doložka o hmotné odpovědnosti.

Každá osoba pověřená zpracováním si je plně vědoma významu a důležitosti pojmu ochrany bezpečnosti osobních údajů a je seznámena s možnými smluvními opatřeními v případě porušení této povinnosti.