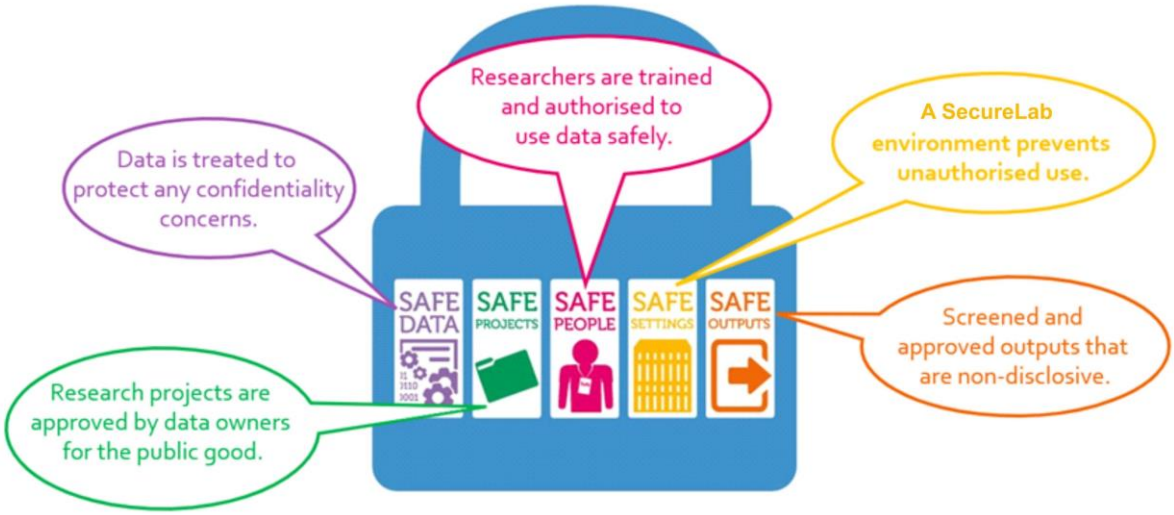
Charta pracovní skupiny Citlivá data

Verze 1.0 z 22.1.2024; vypracoval vedoucí a kolektiv pracovní skupiny.

1 Úvod

Pracovní skupina (PS) je zaměřená na řešení problematiky správy osobních údajů a citlivých dat (různého stupně citlivosti) v digitálním prostředí. Definice a klasifikaci citlivých dat je uvedena jako Příloha 1 tohoto dokumentu.PS se zabývá mapováním stávající situace v ČR, existujícími postupy FAIRifikace citlivých dat a optimalizací kompletní správy těchto dat nezávisle na oboru a s přihlédnutím na stupeň citlivosti. Ke vzniku této skupiny vedla především potřeba standardizace správy citlivých dat napříč vědními obory v ČR. Skupina je v rámci implementace EOSC v ČR skupinou průřezovou, protože citlivá data nejsou součástí pouze jedné vědní domény. Zaměření a okruhy témat řešené touto pracovní skupinou jsou především určované eticko-právními a organizačně-zabezpečovacími aspekty. Doporučení expertů z PS Citlivá data se zohlední v rámci implementace EOSC v ČR a v Národní repozitářové platformě. Tato doporučení by měla pokrýt správu různých typů citlivých dat různého stupně citlivosti.

Od začátku svého působení (duben 2022) se členové PS inspirují řešením UK Data Service – framework 5 safes1 (Obr. 1). V současné době jsou členové PS zapojení do různých *projektů a iniciativ zabývajících se problematikou sdílení citlivých dat.*



Obrázek 1: The Five Safes framework, převzato z https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/, upraveno.

2 Cíle

1. Specifikace požadavků na správu citlivých dat – zaměřeno na digitální prostředí.
2. Definice kroků a úkolů k naplnění specifikací.
3. Dělba úkolů dle odbornosti a zkušeností.
4. Identifikace oblastí, kde je expertíza PS nedostatečná a oslovení dalších expertů ke spolupráci.

3 Výstupy a jejich aplikace

1. Příprava prostředí pro správu citlivých dat napříč oborovými clustery v rámci EOSC CZ.
2. Koordinace, doporučení technologie, odborné týmy podporující správu citlivých dat v rámci EOSC CZ – spolupráce především s PS Vzdělávání a lidské zdroje.

4 Členství a předpokládaní členové

PS je otevřena všem zájemcům o členství se zkušenostmi v oblasti práce s citlivými vědeckými daty. Počet členů pracovní skupiny není omezen. Typicky jsou členy odborníci, kteří s citlivými daty nakládají a/nebo se zabývají jejich správou a ochranou z hlediska technického nebo právního či etického. Skupina spolupracuje s relevantními infrastrukturami a projekty na národní a mezinárodní úrovni.

Pro přihlášení se do PS je třeba vyplnit registrační formulář na webu *https://www.eosc.cz*.

Příloha 1: Vymezení pojmu citlivých dat

Definice

Citlivými daty rozumíme data, na která jsou obvykle kladena následující omezení:

1. Jsou určená striktně jen pro vnitřní potřebu přesně definované skupiny osob (např. zdravotník a jeho pacient, řešitelé projektu pracující s daty podléhajícími komerčnímu či podobnému tajemství apod.);
2. vyžadují ze své povahy zvláštní regulaci, obzvláštní nebo konkrétní specifickou ochranu, typicky jsou explicitně chráněná ze zákona nebo na základě obchodního tajemství, smlouvy, licence apod. (jedná se např. o velmi cenná data spadající pod obchodní tajemství, citlivé osobní údaje zaměstnanců/klientů instituce apod.);
3. jejich zpřístupnění mimo danou skupinu oprávněných osob velmi pravděpodobně způsobí škodu (finanční, morální, právní, na lidském zdraví/životě apod.) značného rozsahu se závažnými/nevratnými následky.

Zařazení do kategorie citlivých dat stanovuje vlastník dat, pokud není určeno jinak zákonem.

Intuitivní definice

Intuitivně jsou to data, u kterých se jejich vlastník domnívá, že by pro jejich ochranu neměl používat jen opatření, která pro ochranu svých dat běžně využívá, ale měl by zavést opatření dodatečná, na nejvyšším dosažitelném stupni ochrany dle soudobé dobré praxe a dostupných technologií, protože tato data jsou v nějakém ohledu výjimečná – mají výjimečnou hodnotu pro jeho činnost; společností jsou všeobecně považovaná za velmi důvěrná; jsou výnosně komerčně využitelná, přitom nedostupná většině zájemců o ně apod.

Posuzování citlivosti dat

Výše uvedenou definici je třeba chápat v kontextu konkrétních dat, jejich vlastníka/správce a nákladů na zavedení ochranných opatření. Obecným pravidlem by mělo být, že vynaložené úsilí a prostředky na ochranu dat by měly být přiměřené škodě způsobené jejich únikem. Je přitom ovšem nutné zohlednit i to, že škody nemusí být jen finanční, ale mohou být také právní, na dobré pověsti organizace apod., což následně může generovat sekundární finanční následky (např. ztrátu důvěry zákazníků, a tudíž pokles příjmů firmy apod.).

Při posuzování škody velkého rozsahu je třeba posouzení vztahovat na konkrétního vlastníka dat a jeho situaci. Finanční škoda 10 mil. Kč může být velkého rozsahu pro malou firmu nebo soukromého podnikatele s ročním obratem 3 mil. Kč, ale nebude velkého rozsahu pro nadnárodní korporaci s ročním obratem v řádu miliard €. Na druhou stranu může být škoda na dobré pověsti organizace způsobená únikem daných dat ve stejném případě neakceptovatelná pro danou nadnárodní korporaci, zatímco pro menší firmu bude mít menší dopad než škoda finanční.

Potenciální škodu na dobré pověsti organizace či fyzických osob je třeba určovat v konkrétním případě a s přihlédnutím k aktuálnímu stavu vývoje techniky a lidského poznání. Je nutné posuzovat, zda je užívána soudobá dobrá praxe, která nezavdá příčinu k závěru, že únik dat byl způsobený nedbalostí nebo zjevným podceněním ochrany dat vlastníkem/správcem. Obdobně bude zpravidla postupováno také při posuzování případných právních důsledků úniku dat, kdy pro některé typy dat může být vyžadováno využívání konkrétních opatření (např.

konkrétní schválené šifrovací algoritmy, certifikované přístroje pro zpracování apod.) nebo aplikace opatření definovaných jako „soudobá nejlepší praxe“.

Kategorie citlivosti dat

Vzhledem k relativnosti posuzování citlivosti dat je definováno několik stupňů citlivosti dat.

Nízká citlivost

Tato třída dat představuje malé nebo žádné riziko pro jednotlivce, soukromé organizace nebo vládní agentury, když jsou data zveřejněna. K datům v této skupině má přístup kdokoli, protože jejich přístupnost je omezena jen málo nebo vůbec. Jde víceméně o veřejnou informaci, o které lze diskutovat kdekoli a s kýmkoli. Příklady zahrnují informace z adresáře zaměstnanců školy, publikované výzkumy, návrhy výzkumu, informace, které jsou již dostupné ve veřejných doménách, a také nepublikovaný výzkum sdílený se svolením výzkumníka, popřípadě zadavatele.

Patří sem veřejná data (například prezentace z veřejných přednášek; veřejně přístupné výzkumné zprávy; open-source software; veřejná výzkumná data; veřejné plány správy dat; veřejné postery) a interní data (Interní korespondence; zápisy z jednání; vnitřní regulace a předpisy; popis metod výzkumu; nedokončené/nepublikované výzkumné zprávy).

Střední citlivost

Střední citlivost zahrnuje údaje, které jsou diskrétní, jsou předmětem smluvního závazku chránit. To znamená, že únik takových dat by způsobil dotčeným jednotlivcům nebo organizacím újmu (finanční, morální, právní), která však nebude mít závažné následky. Příklady středně citlivých údajů zahrnují informace o plánech budov, záznamy o jednotlivých dárcích, záznamy o studentech, duševním vlastnictví, informace o službách IT, víza a další cestovní dokumenty, rozsáhlé kolekce dat s nízkou citlivostí, bezpečnostní informace a kontaktní informace a dokumenty.

Vysoká citlivost / důvěrné údaje

Vysoce citlivá a důvěrná data musí být chráněna zákonem nebo jinými zásadami, které se na ně vztahují. Pokud dojde k jejich zpřístupnění mimo danou skupinu oprávněných osob, může to způsobit škodu (finanční, morální, právní) velkého rozsahu se závažnými následky jednotlivci nebo organizaci. Příklady mimo jiné zahrnují: osobní identifikační údaje, rodná čísla, kontrolované neutajované informace, identifikovatelný výzkum lidských subjektů, údaje o půjčce, chráněné zdravotní údaje, rozsáhlé kolekce dat se střední citlivostí atd. Může také zahrnovat důvěrné firemní informace, jako je jako obchodní tajemství a údaje o duševním vlastnictví, analýze trhu, finanční dokumenty a dokumenty představenstva. Příklady vysoce citlivých dat mohou být:

- Zdravotní data, citlivé osobní údaje (údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení; členství v odborech; genetická data, biometrická data zpracovávaná za účelem identifikace lidské bytosti; údaje týkající se zdraví; údaje týkající se sexuálního života nebo sexuální orientace osoby apod.);
- osobní a ekonomické údaje o zaměstnancích, studentech, zákaznících apod.;
- velmi cenná výzkumná data (poskytující např. unikátní a těžko opakovatelnou konkurenční výhodu, mající potenciál úspěšné komercializace např. formou patentu

apod.) nebo výzkumná data obsahující vysoce důvěrné údaje (chráněné např. na základě právní smlouvy se stanovenými vysokými pokutami apod.),

- obecně tedy data povahy chráněného duševního vlastnictví, obchodního tajemství apod.;
- dosud nepublikovaná výzkumná data, která ještě nebyla využita jejich autory (potenciální škoda finanční [patent apod.]), nebyla dostatečně ověřená jejich správnost (potenciální škoda na pověsti) apod.;
- data citlivá z hlediska kybernetické bezpečnosti (tj. data, jejichž zpřístupnění nepovoleným osobám může např. snížit účinnost opatření IT bezpečnosti nějaké organizace, v důsledku čehož mohou vzniknout škody únikem dat organizace, omezením funkčnosti její IT infrastruktury apod.);
- data, jejichž obecná dostupnost může snížit bezpečnost státu.