Rexel
skartování

Proč je bezpečnost tištěných dokumentů nedílnou
součástí dodržování GDPR.

O tomto dokumentu

Tato bílá kniha vám poskytne **všeobecný přehled o tom, čeho se GDPR snaží dosáhnout**, a o problémech, které toto nařízení může pro firmy představovat, a předkládá rámec řešení, jež firmy mohou v rámci dodržování GDPR přijmout.

Záměrem tohoto dokumentu je představit vám Obecné nařízení EU o ochraně osobních údajů (GDPR) a ukázat, jak toto nařízení ovlivní různé firmy. Vy tak budete moci vytvořit rámec pro firemní politiku bezpečnosti tištěných materiálů ještě předtím, než toto nařízení vstoupí v květnu 2018 v platnost.

Co je to vlastně GDPR? Toto nařízení po firmách vyžaduje, aby zavedly bezpečnostní opatření na ochranu údajů uchovávaných v elektronické i tištěné podobě, a ukládá jim povinnost upozornit dotčené nebo potenciálně dotčené osoby, pokud dojde k narušení bezpečnosti jejich osobních údajů. GDPR se celosvětově vztahuje na všechny firmy, které spravují nebo zpracovávají osobní údaje osob v EU, pokud lze na základě takových údajů příslušnou osobu identifikovat, a to bez ohledu na to, ve které zemi taková firma působí. Požadavky GDPR se vztahují na osobní údaje uložené v elektronické i tištěné podobě a z nařízení vyplývá, že se jím musí řídit všechny firmy, které nakládají s osobními údaji, jež mají původ v EU a z nichž lze člověka osobně identifikovat.

Většina firem již považuje bezpečnost elektronických údajů za samozřejmou, avšak mnoho z nich se příliš nevěnuje osobním údajům v tištěné podobě. Dokonce téměř dvě třetiny úřadů přiznávají, že neprovádí skartaci papírů s důvěrnými informacemi[1]. Značka Rexel jako lídr ve výrobě skartovacích strojů proto doporučuje firmám, aby přehodnotily svou bezpečnostní politiku a praxi ohledně nakládání s osobními údaji v elektronické i tištěné podobě.

OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Přehled

Záměrem GDPR je chránit právo jedinců pobývajících v Evropě na soukromí, a to ať už jsou občany EU, či nikoli. Mezi tato práva na ochranu soukromí patří mimo jiné:

Transparentnost
Právo získat jasné informace o tom, jak firmy nakládají s mými osobními údaji.

Souhlas
Právo kontrolovat, jak firmy používají mé osobní údaje.

Bezpečnost
Právo mít informace o tom, jak firmy adekvátně chrání osobní údaje.

Omezení shromažďování a využití údajů
Právo očekávat, že firmy budou shromažďovat a používat informace v co nejmenší míře.

Upozornění na narušení bezpečnosti
Právo být informován v případě narušení bezpečnosti údajů.

GDPR je součástí plánu Evropské komise na to, že zmodernizuje a sjednotí pravidla týkající se ochrany údajů.

Ačkoli GDPR cílí hlavně na posílení práva na ochranu soukromí na internetu, týká se i ochrany údajů v tištěné podobě.

Zaměřuje se na stále náročnější výzvy v oblasti ochrany osobních údajů a soukromí, narušení bezpečnosti údajů, jejich vystavení hackerským útokům a jiného nezákonného nakládání.

OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Co se mění?

Následující body **představují konkrétní oblasti Obecného nařízení o ochraně osobních údajů, které vytváří nová** práva jedinců nebo posilují již existující práva vycházející ze Zákona o ochraně osobních údajů:

Přenosnost údajů a právo být zapomenut

- Jedinci nyní mají právo převádět své osobní údaje z jedné firmy do jiné.
- Osobní údaje musí být poskytovány ve strukturované a strojově čitelné podobě.
- Každý jedinec může požádat o vymazání nebo odstranění svých osobních údajů.

Upozornění na narušení bezpečnosti údajů

- Jakékoli narušení se musí hlásit dohlížejícímu úřadu.
- Jedinci, kteří se stanou obětí takového narušení bezpečnosti, na ně musí být také upozorněni.

Soupis

- Místním úřadům se již nemusí oznamovat zpracovávání osobních údajů.
- Firmy si musí vést záznamy o úkonech spojených se zpracováním údajů, na které se vztahují tyto povinnosti.

Posouzení vlivu na ochranu osobních údajů

- Díky posouzení vlivu na ochranu osobních údajů je možné zjistit, kde hrozí právům na soukromí jedince vysoké riziko.
- Požadavky a doporučení týkající se bezpečnosti musí být založeny na vyhodnocení rizik.

Správa dat a zodpovědnost

- Firmy musí být také schopny prokázat dodržování GDPR.

Nedodržování požadavků stanovených GDPR může mít za následek **udělení pokuty ve výši až 20 milionů eur nebo 4 % celosvětových příjmů společnosti, přičemž je uplatňována vyšší částka. Subjekt, jehož se údaje týkají, má navíc právo firmu žalovat.**

OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Na koho se vztahuje?

Zavedení GDPR v květnu 2018 se dotkne těchto pracovních pozic:

Správci údajů – určují, jak a proč jsou osobní údaje zpracovávány
Zpracovatelé údajů – lidé pracující podle pokynů správců údajů

Zodpovědností osob na těchto dvou pozicích je zajistit, aby jejich klienti bezvýhradně dodržovali veškerá opatření uvedená v GDPR, jinak jim může být vyměřena pokuta.

Zpracovatel údajů **musí stanovit pověřence pro ochranu údajů** a vést záznamy o veškerých aktivitách spojených se zpracováním údajů, které jsou prováděny jménem jeho klientů.

GDPR se vztahuje na osobní údaje a citlivé osobní údaje v elektronické i fyzické podobě

Než vytvoříte politiku pro vaši firmu, je důležité zamyslet se nad tím, na jaké druhy údajů se GDPR vztahuje.

Jakých údajů se GDPR týká? Jakýchkoli informací o identifikovatelné osobě.
Mezi osobní údaje, na něž se GDPR vztahuje, patří například celé jméno, e-mailová adresa nebo telefonní číslo.

GDPR se týká také doplňující ochrany **podkategorie osobních údajů nazývaných citlivé osobní údaje**.

GDPR se vztahuje na osobní údaje, se kterými firmy nakládají v **elektronickém i fyzickém formátu**, jako jsou například tištěné dokumenty.

Firemní rámec dodržování GDPR

Aby firmy dosáhly souladu s GDPR, musí přehodnotit tři hlavní oblasti. Pokud se na ně zaměří, budou schopné vytvořit jasný rámec zabezpečení údajů v každém aspektu a splní tak všechny požadavky GDPR.

Těmito třemi oblastmi jsou:

Lidé

Pracovní povinnosti a zodpovědnosti zaměstnanců za jakékoli údaje, které firma zpracovává, jsou zde klíčové. Firma musí pro každého zaměstnance stanovit jasná pravidla správného nakládání s elektronickými i tištěnými údaji, které má firma v držení.
Taková opatření uvedou v praxi požadavky GDPR týkající se nakládání s údaji. Mezi tato pravidla může patřit například jasné stanovení toho, jak se smí používat tištěné dokumenty obsahující citlivé informace, nebo správného procesu jejich skartování podle toho, jak citlivé jsou údaje, které dokument obsahuje.

Postupy

Zde máme na mysli firemní postupy, například management používání údajů o zákaznících, tedy jejich zpracování či ukládání. Je zcela zásadní, aby firmy přehodnotily všechny své současné postupy týkající se údajů. Poté, co určí mezery a slabé stránky existujících postupů, je nutné vytvořit rámcový plán, který takové oblasti posílí nebo v případě potřeby nahradí některý proces jiným tak, aby firma dodržovala opatření uvedená v GDPR.

Technologie

Posoudit by firmy měly i současnou způsobilost svých informačních technologií a požadavky na ně a před květnem 2018 je přizpůsobit potřebám nařízení. Je na každé jednotlivé firmě, aby zajistila výměnu nebo úpravu současných systémů, pokud plně nevyhovují požadavkům nařízení. Tím se vyhne případným pokutám poté, co vstoupí GDPR v platnost.

Proč záleží i na bezpečnosti tištěných dokumentů?

Z výše uvedených požadavků GDPR vyplývá, že je nezbytné zaměřit se ve firmě i na bezpečnost tištěných dokumentů, protože ta je pro dodržování požadavků GDPR klíčová.

Ze zprávy z roku 2014, zpracované společností PwC ve spojení s Iron Mountain (firma zabývající se správou údajů)[2], která zkoumala, jak středně velké podniky v Evropě vnímají informační rizika a jejich management, vyplývá, že dvěma třetinám dotazovaných firem dělalo řízení rizik spojených s tištěnými materiály velké starosti.

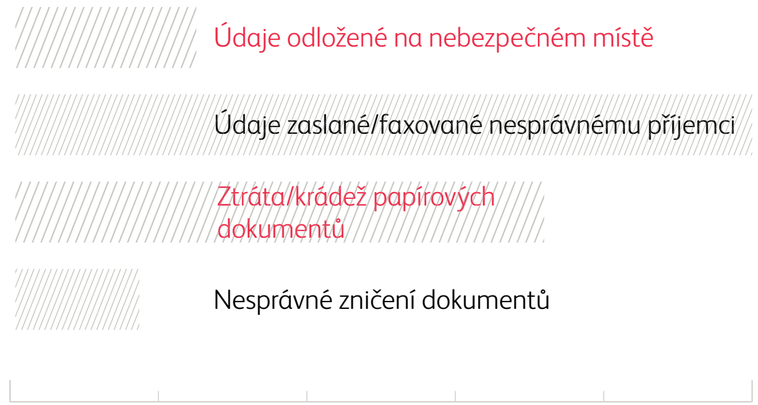
V centru zájmu firem jsou sice nyní hlavně digitální hrozby, avšak bylo by chybou domnívat se, že ***rizika spojená s tištěnými dokumenty*** *už pominula.*

Při zacházení s tištěnými dokumenty se stále porušují bezpečnostní opatření

Z 598 případů porušení bezpečnosti, které mezi červencem a zářím 2016 zaznamenal britský úřad na ochranu údajů ICO, bylo:

14 % způsobeno ztrátou nebo krádeží tištěných dokumentů, **19 %** zasláním poštou či faxem nesprávnému příjemci **a 4 %** tím, že byly dokumenty ponechány na nebezpečném místě. **Další 3 %** byla způsobena nesprávnou likvidací papírů. Navzdory exponenciálním nárůstu digitálních technologií tedy měly **40 % incidentů** na svědomí dokumenty v papírové podobě[3].

40 % **bezpečnostních incidentů v Británii se týkalo tištěných dokumentů**



Zaznamenané bezpečnostní incidenty s tištěnými dokumenty

Spolupráce uživatelů je při dodržování GDPR klíčová

Pokud chceme vyslovit závěr, že bezpečnost papírových dokumentů zůstává pro informační bezpečnost zcela zásadní, vyvstává následující otázka: Co v této věci mohou firmy udělat?

Značka Rexel se specializuje na firemní skartovačky papírů a spolupracuje při tom s takovými společnostmi, jako je například Kensington, světový lídr v oblasti fyzické bezpečnosti IT hardwaru. Díky tomu dobře chápe, jakým výzvám čelí firmy při hledání řešení, jež by jim pomohlo dodržovat požadavky GDPR.

Zjistili jsme, že efektivní skartování dokumentů čelí ve firmách dvěma hlavním překážkám:

Nedostatek povědomí

Firmy vzhledem k narůstajícímu podílu digitálních technologií na pracovišti přehlíží důležitost papíru a otázkám zabezpečení papírových dokumentů věnují málo času. I v případech, kdy ve firmě platí politika bezpečnosti, se může stát, že se o těchto pravidlech nekomunikuje efektivně, takže o nich zaměstnanci nemají dostatečné povědomí.

Snadnost použití

Dostupnost vhodných skartovaček je pro úspěch bezpečnostní politiky v oblasti tištěných dokumentů zcela zásadní. Firmy či úřady se často spoléhají na nevýkonné manuální skartovačky, které nemají potřebnou kapacitu. Zaměstnanci pak nemohou efektivně a produktivně skartovat nepotřebné dokumenty.

V návaznosti na zavedení účinné politiky skartování dokumentů ve firmě je dalším krokem stanovit účinné řešení pro překonání těchto překážek.

Řešení č. 1 pro splnění požadavků GDPR

Dostatek povědomí

Zaměstnanci obecně provádí ty úkony, které jejich vedoucí zdůrazňují jako priority.

V souvislosti s tím může jasná a pevná politika skartování udělat hodně.

Zpráva PwC / Iron Mountain z roku 2014 informující o středně velkých podnicích v Evropě udává, že pouze 40 % společností má pro zaměstnance jasné směrnice k internímu likvidování a ukládání fyzických dokumentů a pouze 27 % má firemní politiku zabezpečení, bezpečného skladování a bezpečného likvidování důvěrných informací.

Řešení č. 2 pro splnění požadavků GDPR

Snadnost použití

Druhou nejčastější příčinou, proč zaměstnanci nedodržují pravidla skartování dokumentů, je obtížnost a časová náročnost tohoto úkolu.

I když mají zaměstnanci přístup ke skartovačkám, ne všichni vždy příslušné dokumenty skartují, a to především proto, že je to stojí hodně času či námahy.

Nikoho nepřekvapí, že společnosti nejsou ochotné investovat do skartovaček, které pak zaměstnanci kvůli jejich nízké výkonnosti nebo špatné ovladatelnosti nepoužívají. Aby byly skartovačky maximálně využívány, je třeba věnovat těmto problémům pozornost.

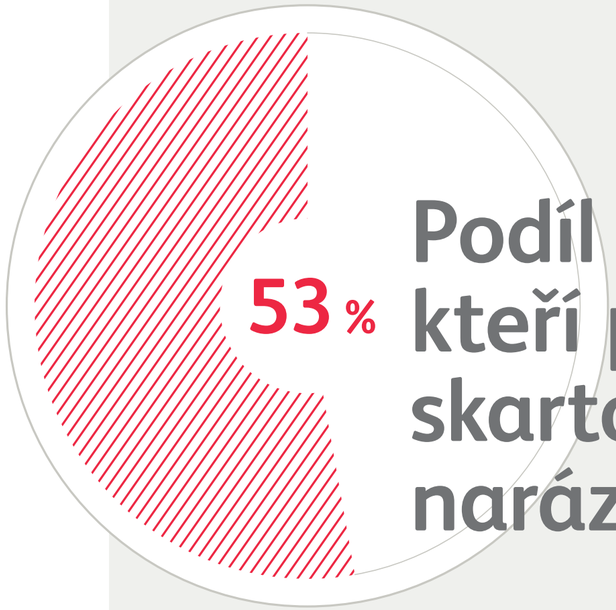
Zvýšení produktivity zaměstnanců díky technologii Auto Feed

Závěr:

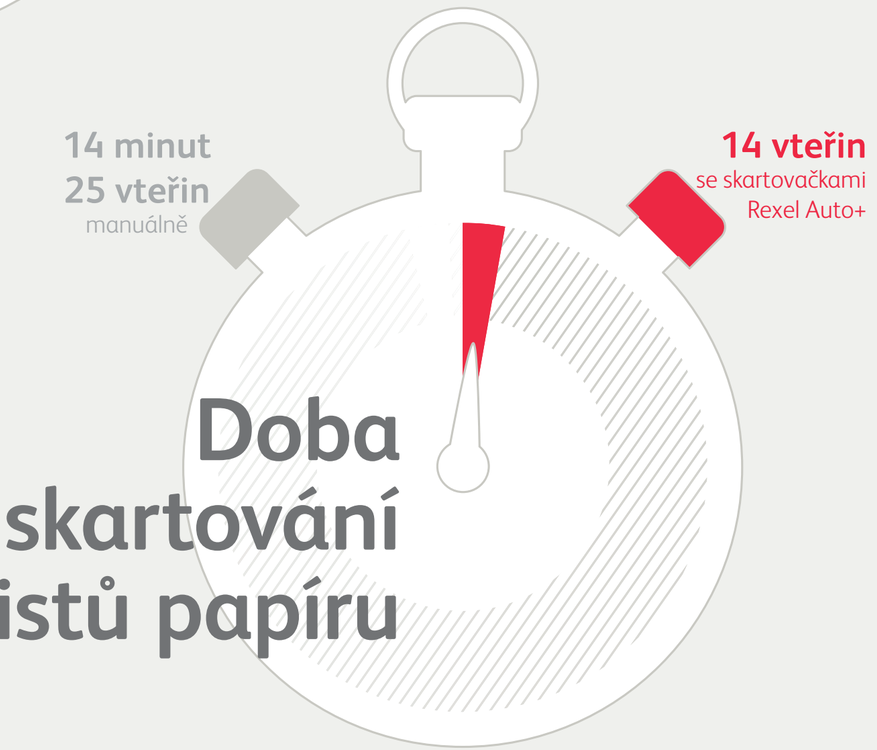
Skartovačky papíru s technologií Auto Feed jsou přímou odpovědí pro firmy, které potřebují motivovat zaměstnance, aby dodržovali pravidla zabezpečení tištěných dokumentů.

Náš průzkum[4] ukazuje, že 53 % zaměstnanců preferuje skartování více listů naráz, takže nejprve počkají, až se jim nashromáždí více dokumentů, aby se jim cesta ke skartovačce vyplatila.

Pokud zaměstnancům umožníte skartovat více listů naráz, **stráví podle nezávislého výzkumu skartováním o 98 % méně času**[5] a mají tendenci skartovat dokumenty častěji.



Podíl zaměstnanců, kteří preferují skartování více listů naráz



Doba skartování 500 listů papíru

Šestibodový akční plán GDPR pro vaši firmu

1. Určení pověřence pro ochranu údajů

Tento pověřenec musí být plně srozuměn s povinnostmi firmy v oblasti dodržování GDPR a musí vědět, jaké údaje jsou ve vaší společnosti označovány jako „osobní“, kam se ukládají, kdo k nim má přístup, jak zaregistrovat narušení jejich bezpečnosti a komu ho nahlásit. **Pověřenec pro ochranu údajů nemusí být zaměstnancem firmy – můžete zde využít outsourcing.**

2. Vyhodnocení vašich systémů

Proveďte revizi všech smluv, technologické podpory, procesů a nástrojů na zpracování, nakládání, ukládání a mazání údajů. Pomůže vám to určit mezery a slabá místa, která vyžadují změny.

3. Vyvinutí strategie

Vytvořte novou strategii, která zajistí, že vaše společnost bude dodržovat veškerá nařízení GDPR. Taková strategie může představovat nové investice do technologií, přehodnocení pracovních procesů zaměstnanců a vytvoření nových pracovních rolí.

4. Zavedení nové firemní politiky

Dalším krokem k dodržování GDPR je zavést plán do praxe na všech úrovních firmy. Investujte do zavedení nových technologií na pracovišti a vydejte informační příručku pro zacházení s údaji a jejich zpracování.

5. Angažovanost zaměstnanců

Zaveďte novou politiku dodržování pravidel o ochraně údajů, platnou pro všechny zaměstnance. Poskytněte jim proškolení, informační příručky a rady, aby měli znalosti a povědomí o změnách a vlastních povinnostech v rámci dodržování požadavků GDPR.

6. Revize a zlepšování

Po spuštění plánu dodržování GDPR a ještě před vstupem GDPR v platnost proveďte revizi jeho dodržování a učiňte kroky ke zlepšení. Identifikujte oblasti, kde je nezbytné se zlepšit, s dostatečným předstihem před květnem 2018, kdy GDPR vstoupí v platnost, abyste měli jistotu, že se do té doby účinně a úspěšně přizpůsobíte všem změnám a dokážete GDPR dodržovat.

Zdroje

1 envirowaste.co.uk/blog/articles/third-companies-shred-private-documents

2 Beyond good intentions: The need to move from intention to action to manage information risk in the mid-market, PwC report in conjunction with Iron Mountain, June 2014.

3 ico.org.uk/action-weve-taken/data-security-incident-trends

4 Evaluating Auto Feed Shredders. Prepared for ACCO Brands by Deep Blue Insight

5 Nezávislý test Intertek Testing & Certification Ltd, červen 2012.
Maximální úspory při používání Auto+ 500X v porovnání s tradičně plněnými skartovačkami podobné cenové hladiny.
Průzkum ukázal, že manuální vložení 500 listů papíru do tradiční manuálně plněné skartovačky trvá v průměru 14 minut a 25 vteřin, ale vložení stejného počtu listů do skartovačky Auto+ 500X trvá pouze 14 vteřin.