Co jste chtěli vědět o GDPR a nestačili se zeptat...

GFI Software™

Prosinec 2017

GFI Software™

Obsah

GFI Software™

Úvod a shrnutí

Obecné nařízení o ochraně údajů (GDPR) bylo parlamentem Evropské unie zavedeno do právního řádu v dubnu 2016 a jeho vstoupení v platnost bylo stanoveno na 25. května 2018. S rychle se blížícím termínem vstoupení v platnost organizacím dochází čas na rozhodnutí, jestli a jak se jich nařízení dotýká, případně jak implementovat změny ve svých IT procesech nutné ke splnění požadavků.

GDPR nahrazuje směrnici o ochraně údajů (směrnice 95/46/EC), která byla základem evropských zákonů o ochraně soukromí od roku 1995. Jako většina vládních nařízení, GDPR je komplexním dokumentem **a v některých ohledech je otevřeno interpretaci.** Úmyslem tohoto právního předpisu je ochrana soukromí občanů EU a standardizace zákonů napříč všemi státy EU.

Dobrou zprávou je, že organizace mají k dispozici mnoho nástrojů, které jim umožní provést a zdokumentovat kroky, jež jsou ke splnění požadavků GDPR nutné; od rozpoznání osobních údajů, které musí být chráněny, po jejich správné zabezpečení, efektivní řízení a sledování jejich pohybu a toho kde, kdy a kdo k nim má přístup.

Poznámka: I když jsme přesvědčeni, že jsou informace obsažené v této Bílé knize přesné, měla by vám sloužit pouze jako pomůcka, nikoli jako právně závazný dokument.

Terminologie GDPR

K porozumění požadavkům kladených GDPR a tomu, jak je dodržovat, je třeba nejdříve pochopit význam určitých klíčových termínů a konceptů, které se v právním předpise vyskytují. Naneštěstí nechává GDPR některé termíny otevřené interpretaci. Například požaduje, aby organizace zavedly „rozumnou“ míru ochrany osobních dat, aniž by byla „rozumná“ míra blíže definována.

Nejen následující termíny jsou definovány v článku 4 nařízení GDPR:

Osobní údaje

Účelem GDPR je ochrana osobních údajů a na rozdíl od předchozí směrnice, termín „osobní údaje“ je v něm přesně definovaný a definice se tak nenechává na jednotlivých členských zemích EU. Definice osobních údajů je v GDPR velmi široká; jsou definovány jako:

Každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

To zahrnuje (ale není vyhrazeno) základní identifikační údaje (jméno, adresa, telefonní číslo, identifikační čísla), biometrické údaje, webové údaje (IP adresy, lokace, informace z cookies, údaje z RFID tagů). Rasové nebo etnické údaje, sexuální orientace, členství v obchodní unii, politické názory a náboženská víra jsou klasifikovány jako speciální kategorie neboli „citlivé osobní údaje“ a jsou předmětem dodatečné ochrany.

GFI Software™

Údaje, které jsou úplně anonymizovány tak, aby jednotlivci nemohli být identifikování přímo či nepřímo, jsou ze záběru GDPR vyřazeny.

Pseudonymizace

Pseudonymizované údaje jsou odlišné od anonymizovaných údajů.

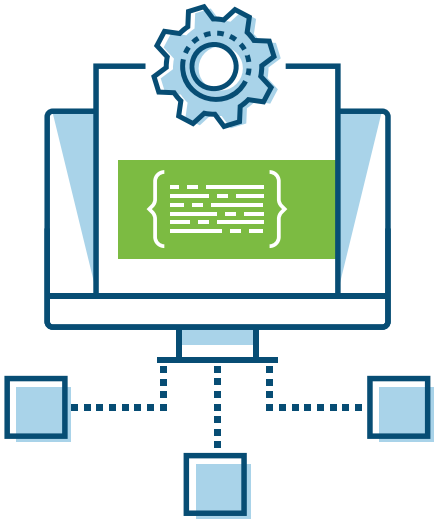
Pseudonymizace může být i pro mnoho IT profesionálů novým termínem; znamená:
Zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů ***bez použití dodatečných informací,*** *pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.*

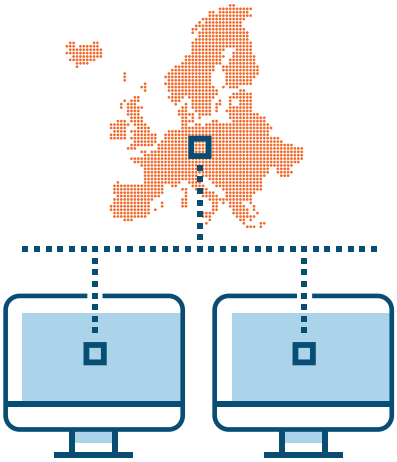
Pseudonymní údaje jsou stále považovány za osobní údaje, mohou ale vyžadovat menší míru ochrany.

Zpracování osobních údajů

GDPR ukládá dodržování požadavků k ochraně údajů během jejich zpracování, které je definováno jako:
Jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů.

Definice pokrývá širokou škálu činností, které zahrnují téměř vše, co se s osobními údaji dá dělat: shromažďování, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení údajů.





Správci a zpracovatelé

GDPR se vztahuje na organizace, které sbírají, ukládají a/nebo zpracovávají osobní údaje evropských občanů. Na obě skupiny se vztahují povinnosti dodržovat nařízení; nicméně, GDPR přiřazuje rozdílnou zodpovědnost na základě dvou rolí, které může organizace hrát.

Pod GDPR, osoba nebo organizace, která samostatně nebo *společně s dalšími rozhoduje o účelech a prostředcích zpracování osobních údajů,* je nazývána správcem. Osoba nebo organizace, která osobní data pro správce zpracovává, je nazývána zpracovatelem. Stejná organizace může fungovat jako správce pro některé údaje, a jako zpracovatel pro údaje jiné.

GFI Software™

Přehled o GDPR

První otázkou, kterou si musí každá organizace s ohledem na GDPR zodpovědět, zní „týká se nás“? GDPR oproti předchozí směrnici rozšiřuje svou extrateritoriální uplatnitelnost.

Pokud má vaše organizace sídlo v EU a je správcem nebo zpracovatelem, odpověď zní ano, a to i když údaje nejsou v EU zpracovávány. Nicméně i když vaše organizace nemá sídlo v EU (není v EU fyzicky přítomna), ale i tak poskytuje zboží nebo služby uvnitř EU nebo občanům EU nebo monitoruje chování občanů EU, je rovněž povinna nařízení GDPR dodržovat.

Další oblasti, ve kterých se zákony zpřísňují:

- Povinné upozornění na narušení do 72 hodin od prvního zjištění narušení.
- Právo subjektů údajů na žádost o zastavení zpracování nebo šíření osobních údajů a výmaz údajů v případě, že subjekt odvolá svolení nebo pokud už údaje nejsou relevantní (také známo jako „právo být zapomenut“).
- Právo subjektů údajů na obdržení kopie svých osobních údajů v běžném elektronickém formátu, v případě žádosti, a právo je předat jinému správci.
- Pravidla pro získání svolení od subjektů údajů nyní vyžadují jasný a jednoduchý jazyk (konec matení mořem právničiny) a odvolání souhlasu musí být snadné.
- „Soukromí již od návrhu“ vyžaduje, aby byla ochranu údajů zabudována do systémů už od fáze návrhu.

Velmi důležitý rozdíl mezi předchozí směrnicí o ochraně údajů a nynějším obecném nařízení o ochraně údajů leží v názvech: první je směrnicí, druhé je nařízením. Směrnice mohou být interpretovány a implementovány v rozličných zemích EU různě. Nařízení je vynutitelným právem, které má být vykládáno a aplikováno jednotně napříč celou EU.

Pro úplné porozumění GDPR je třeba přečíst jak články (přijatý zákon), tak jejich body odůvodnění, které vytyčují důvody pro ustanovení zákona a pomáhají s interpretací jeho významu. GDPR sestává z 99 článků a 173 bodů odůvodnění.

Dopad GDPR

Mnoho společností mimo EU, které dříve nespadaly pod směrnici o ochraně dat, bude muset nově dodržovat GDPR kvůli výše zmiňovanému rozšíření uplatnitelnosti. Například „monitoring chování“ může zahrnovat využívání cookies k profilování občanů EU na webových stránkách.

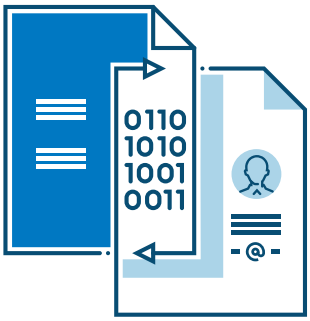
Mnoho organizací bude nuceno změnit způsob, jakým sbírají, skladují, zpracovávají a chrání informace o svých zákaznících. Společnosti, které spadají pod GDPR, musí posoudit své možnosti a vypracovat strategii pro soulad. Například se musíte rozhodnout, jestli implementovat stejná ochranná opatření pro všechny osobní údaje anebo mít oddělené postupy pro občany EU.

Některé organizace budou nově nuceny jmenovat inspektora ochrany údajů (DPO z Data Protection Officer). To se týká jak správců, tak zpracovatelů, pokud je součástí jejich hlavních aktivit zpracování, které vyžaduje rozsáhlé, pravidelné a systematické sledování subjektů údajů. Tato nová povinnost se rovněž vztahuje na ty, kteří sbírají nebo zpracovávají speciální kategorie údajů nebo údaje související s trestnými činy a s odsouzeními. DPO musí být kvalifikovaným expertem v postupech a zákonech o ochraně údajů. Úkoly DPO jsou vypsány v článku 39.

Důsledky nedodržení GDPR mohou být přísné; tresty se mohou lišit podle povahy porušení, ale maximální pokuta je **vyšší částka** ze 4 % ročního globálního obratu, nebo €20 milionů. Americké společnosti utrácejí miliony dolarů, aby se těmto pokutám vyhnuly a aby splňovaly požadavky nařízení GDPR.

Požadavky GDPR

Než budou moci IT experti pracující pro správce a zpracovatele začít implementovat řešení, která jejich organizacím pomohou splňovat požadavky GDPR, je důležité, aby věděli, jaké požadavky to jsou. GDPR požadavky mohou být rozděleny do několika širokých kategorií, které se ale mohou vzájemně překrývat.



Identifikace a klasifikace osobních údajů

Logickým prvním krokem k ochraně osobních údajů je jejich identifikace a rozlišení od ostatních dat, která společnost ukládá a zpracovává. To znamená implementaci nové **strategie pro klasifikaci údajů** nebo aktualizaci té již existující. Klasifikaci údajů, zahrnující nalezení a označení osobních údajů a citlivých osobních údajů, už mnoho organizací v rámci vlastní globální bezpečnostní strategie provádí.

Implementace plánu správy osobních údajů

Správou údajů se rozumí zásady a procedury řízení a zpracování údajů, spolu s plánem implementace daných zásad a procedur. Účelem by mělo být zajištění jednotně řízeného zpracovávání údajů napříč organizací.
Slovy Data Governance Institute:

„Správa údajů je systémem rozhodovacích práv a odpovědností nad informacemi, týkajícími se procesů, které jsou prováděny v souladu s domluvenými modely, které popisují, kdo může provést jaké akce s jakými informacemi, kdy a za jakých podmínek a za použití jakých metod.“

Váš plán správy údajů je základním prvkem pro splnění požadavků GDPR. Aby požadavkům odpovídal, musí jasně definovat role a zodpovědnosti vůči přístupu, řízení a využití osobních údajů. Procesy a zodpovědnost jsou důležitými prvky strategie správy údajů.

Vytvoření postupů pro řízení osobních údajů

GDPR nastoluje povinnosti pro správce a zpracovatele, kteří mají vliv na způsob řízení osobních údajů od občanů EU. Správci jsou povinni:

- **Získat svolení před zpracováním osobních údajů (když je svolení základem pro zpracování).** Článek GDPR č. 7 žádá, aby bylo svolení vydáno dobrovolně, jako specificky a jednoznačně vyjádřené přání subjektu. Nemůže být odvozeno; subjekty údajů musí provést zřejmou a explicitní akci, aby se přihlásili. Požadavky na svolení ke zpracování údajů, jež jsou klasifikovány jako citlivé osobní údaje nebo jako osobní údaje dětí, jsou přísnější, jak specifikují články 8 a 9.

- **V okamžiku, kdy jsou osobní údaje subjektů dat sbírány, jim musí být poskytnuty konkrétní informace.** Informace musí zahrnovat detaily o identitě a kontaktní informace na správce a (případně) jeho inspektora ochrany údajů, účely, za kterými jsou osobní údaje sbírány a zpracovány, a jestli jsou údaje přenášeny do zemí mimo EU. Správce musí subjekty údajů také zpravit o jejich právech na odvolání souhlasu k použití jejich údajů, na opravu údajů (oprava chyb nebo doplnění informací) a na výmaz osobních údajů. Tyto požadavky jsou vypsány v článcích 15, 16, 17, 19 a 20.

- **Ukončit zpracování osobních údajů.** Pokud subjekt údajů odvolá své svolení, GDPR na správci vyžaduje, aby ukončil zpracovávání, pokud pro něj neexistuje alternativní právní základ. Zákonným základem pro zpracování je pod článkem 6(1), kromě svolení, zpracování nezbytné pro provedení smlouvy se subjektem údajů, zpracování nutné k dodržení zákonné povinnosti, zpracování nutné k ochraně životních zájmů subjektu nebo jiných osob, zpracování nutné k vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci nebo zpracování nutné pro legitimní zájmy správce nebo třetí strany, pokud tyto zájmy nejsou přebity zájmy, právy nebo svobodami subjektu dat. [**Poznámka:** pro speciální kategorie existují dodatečné podmínky].

- **Omezit zpracování osobních údajů na požádání.** Ve specifických situacích, vypsaných v článku 18, může subjekt údajů požádat o dočasné omezení zpracovávání osobních údajů, přičemž ale údaje nemusí být smazány. Taková situace může nastat, když je vyšetřována přesnost údajů, když je zpracování nezákonné nebo když subjekt údajů vznesl námitku proti zpracování a čeká se na ověření důvodů ke zpracování. Pokud byly osobní údaje přeneseny nebo sdíleny s třetí stranou, měla by být také informována o omezení zpracovávání

- **Poskytnout subjektům údajů kopii jejich osobních údajů na požádání.** Podle článku 20 musí správci v určitých podmínkách poskytnout osobní údaje v „strukturovaném, běžně používaném a strojově čitelném formátu“. GDPR rovněž vyžaduje, aby byly osobní údaje na přání subjektu přenášeny dalším správcům „bez překážek“. To znamená, že musíte prokázat schopnost exportovat tyto osobní údaje v běžně používaném souborovém formátu. To je známo jako přenositelnost dat.

Ochrana osobních údajů pomocí bezpečnostních opatření

- **Přijmout obecná i konkrétní bezpečnostní opatření k ochraně osobních údajů.** GDPR na správcích a provozovatelích vyžaduje implementaci „zásady ochrany údajů již od návrhu a standardního nastavení ochrany údajů“ pomocí přiměřených technických a organizačních opatření (článek 25). Implementace může být prokázána schváleným certifikačním mechanizmem (článek 42). Konkrétnější bezpečnostní opatření zahrnují šifrování a pseudonymizaci. V obecnější rovině, článek 32 vyžaduje, aby zpracovatelé prokazovali schopnost zajištění průběžné diskrétnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování a schopnost obnovit dostupnost a přístup k osobním údajům včas v případě fyzického nebo technického incidentu.

- **Provádět testování, posuzování a hodnocení.** Zpracovatelé musí rovněž prokazovat pravidelné testování, posuzování a hodnocení efektivity vlastních bezpečnostních opatření v souladu s článkem 32.

Oznamování, vedení záznamů a ohlašování

- **Oznámit příslušným orgánům dozoru narušení bezpečnosti osobních údajů.** Podle článku 33 jsou správci povinni narušení oznámit do 72 hodin od jeho zjištění. Článek 55 definuje příslušné orgány dozoru.
- **Vést záznamy o prováděném zpracovávání.** Článek 30 správcům a zpracovatelům ukládá povinnost udržovat detailní dokumentaci (audit trail), která prokazuje účely a definuje kategorie prováděného zpracovávání, kategorie příjemců, se kterými osobní údaje byly nebo budou sdíleny a všechny přenosy osobních dat do třetích zemí nebo mezinárodních organizací, časové lhůty pro výmaz různých kategorií údajů, a popisuje implementovaná technická a organizační bezpečnostní opatření. Pro organizace zaměstnávající méně než 250 osob existuje omezená výjimka, pro jejíž přidělení je třeba splňovat přidaná kritéria a mnoho organizací na ni tak nedosáhne. Záznamy musí také zahrnovat sledování toku údajů do zemí mimo EU a k poskytovatelům služeb třetích stran.
- **Vykonávat posouzení dopadu na ochranu údajů (DPIA z Data Protection Impact Assessment).** Zpracovatelé jsou pod článkem 35 povinni provádět DPIA tam, kde zpracování údajů probíhá za pomoci nových technologií a práva a svobody jednotlivců jsou tak vystaveny vyššímu riziku. DPIA je vyžadováno v konkrétních případech, včetně instancí rozsáhlého sledování veřejně přístupných oblastí; hodnocení osobních aspektů fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na jehož základě je rozhodováno a které vytváří legální nebo jiný závažný efekt dotýkající se té osoby; a zpracování, jež se týká speciálních kategorií údajů definovaných v článku 9 a 10 („citlivé osobní údaje a údaje týkající se trestných činů a odsouzení“).

GDPR v cloudu

Přechod do cloudu pro mnohé organizace znamená, že už jejich IT oddělení nemá tak velkou kontrolu nad bezpečnostní dat, jakou disponovalo, když byla všechna data organizace zpracovávána místně. V době zatížené na cloud, kdy jsou hybridní sítě běžnou praxí, bezpečnost je zodpovědností sdílenou **mezi poskytovateli cloudu a jejich zákazníky.**

K zajištění souladu s GDPR v takových případech potřebujete vědět, kde přesně leží vaše zodpovědnost a jaká opatření váš poskytovatel cloudu přijal, aby zabezpečil údaje skladované a zpracovávané skrze jejich služby. Microsoft a Amazon vydali pro jimi poskytované cloudové služby, Azure a AWS, zásady sdílené zodpovědnosti.

Je důležité pamatovat, že i v modelu sdílené zodpovědnosti je vaše organizace tím, kdo může být za nedodržení GDPR nakonec pokutován. Součástí vaší zodpovědnosti je vybrat si správného poskytovatele cloudu a zajistit, aby veškerá nepovinná bezpečnostní opatření, jakými jsou dvoufaktorová autentizace, šifrování nebo silná správa klíčů na vašem účtu, byla v provozu. Nemůžete předpokládat, že uložení vašich dat do cloudu automaticky zaručuje soulad s GDPR.

Jak Microsoft, tak Amazon poskytují svým zákazníkům informace o implementovaných opatřeních a o tom, co jejich služby dělají pro to, aby vám pomohly s dodržováním GDPR.

GFI Software™

GDPR řešení

Poté, co jste získali znalosti o základní terminologii, o dopadu GDPR a o požadavcích, které musí být k dosažení souladu s nařízením naplněny, můžete vyvinout plán implementace. Vaše technická a organizační řešení budou namířena na plnění konkrétních požadavků – a ke splnění všech požadavků bude zapotřebí několika úrovňové strategie.

IT experti se budou nejvíce zajímat o technologické nástroje a bezpečnostní prvky, které mohou být použity k identifikaci, klasifikaci, řízení, zabezpečení, sledování a dokumentování osobních údajů, a které jsou předmětem pravidel GDPR. Naštěstí je zde mnoho řešení, která jste již implementovali v rámci zavádění osvědčených bezpečnostních postupů a která mohou být ke splnění požadavků GDPR dostačující.

V následujících sekcích jsou rozebírány některé z technologických nástrojů, jež vám s dodržováním GDPR pomohou.

Nástroje pro identifikaci a klasifikaci údajů

Řešení, která vám pomáhají identifikovat a označit osobní údaje a citlivé osobní údaje, jež jsou předmětem nařízení GDPR, jsou další kriticky důležitou součástí vaší strategie pro implementaci souladu s GDPR. Existuje mnoho nástrojů třetích stran, které dokáží pomoci a operační systémy, databázový software, služby cloudového ukládání dat a další řešení, která již využíváte, také obsahují za tímto účelem využitelné, zabudované mechanismy.

Například můžete využívat PowerShell skriptů ve Windows, Azure Search v Microsoft cloudu, dotazovací nástroje v SQL Server atd. k vyhledávání údajů na základě struktury nebo vzoru (jako je číslo pojištěnce). Azure Information Protection (AIP), které je součástí řešení Microsoft Enterprise Mobility + Security (EMS) pomáhá klasifikovat údaje na Windows Server souborových serverech a v Active Directory zase můžete vytvářet pravidla pro automatickou klasifikaci údajů.

Amazon nabízí službu Macie, která automatizuje proces nalezení, klasifikace a zabezpečení velkého množství dat uloženého v AWS cloudu. Uživatelská příručka vysvětluje, jak Macie ke klasifikaci dat uložených v AWS S3 bucketech využívat.

Řešení pro šifrování dat

Ochrana osobních údajů zahrnuje šifrování at-rest (kde jsou uložena, byť dočasně) a in-transit (při přenosu po soukromých sítích nebo po internetu). Šifrování zajišťuje, že i když útočníci získají neautorizovaný přístup k vašim uloženým údajům nebo je zachytí při přenosu, nebudou schopni je přečíst.

Řešení pro šifrování at-rest zahrnují šifrování celého disku/svazku a šifrování na úrovni souborů. Technologie jako BitLocker od Microsoftu a Encryption File System (EFS), stejně jako mnoho jiných produktů třetích stran, dokáží zašifrovat celé disky nebo diskové svazky. Správa šifrování přenosných zařízení může být obzvláště obtížná. K rozpoznání úložných zařízení zašifrovaných s BitLocker To Go, k nastavení různých povolení a k šifrování těch zařízení, která nejsou zabezpečena, můžete využít GFI EndPointSecurity.
K šifrování osobních údajů by mělo být používáno silné šifrování, jako je 256-bitové šifrování AES.

Pro šifrování in-transit je standardním protokolem Transport Layer Security (TLS), který poskytuje silnou autentizaci a chrání soukromí a integritu údajů při jejich přenosu po sítích. Osobní údaje in-transit mohou být chráněny využitím šifrovaných tunelů přes VPN připojení. Všechny webové transakce obsahující osobní údaje by měly být chráněny HTTPS. SMB 3.x se SMB šifrováním umožňuje šifrování údajů přenášených přes síť, včetně přenášení mezi virtuálními stroji.

Hlavní poskytovatelé cloudových služeb nabízejí automatické i volitelné šifrovací funkce, které chrání údaje v úložných zařízeních i při přenosu po sítích poskytovatelů, i mezi klienty a jejich datovými centry. Služby Microsoft Azure nabízejí mnoho šifrovacích možností, stejně jako Amazon Web Services (AWS). Obě podporují šifrování na straně klienta i na straně serveru.

Šifrování je bezpečné do té míry, do jaké jsou v bezpečí klíče, na kterých šifrování závisí. Šifrovací klíče by měly být uloženy na zabezpečeném místě a chráněny dobrým systémem správy klíčů.

Správa identit a přístupu

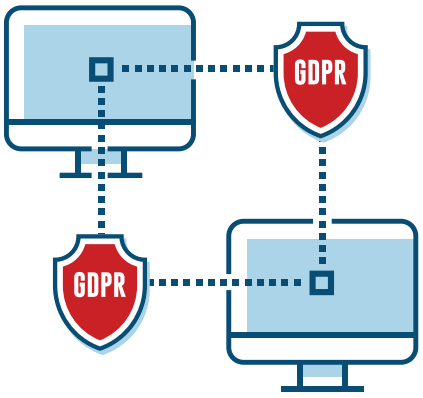
Základem zabezpečení údajů je správa identit. Kontrola přístupu k osobním údajům je nezbytným prvkem pro jejich zabezpečení a ke splnění požadavků GDPR, stejně jako správa identit zákazníků a zaměstnanců. Dobré IAM (Identity and Access Management) řešení je pro organizace nezbytné k identifikaci subjektu, jehož údaje se ukládají a zpracovávají, k identifikaci umístění, ve kterém se údaje nachází a může pomoci se správou svolení a s vyřizováním žádostí subjektů údajů o opravu nebo výmaz a s vytyčováním omezení přístupu k osobním údajům.

Windows Server Active Directory a Microsoft Identity Manager poskytují jednoduché IAM řešení pro on-premises datová centra, ale existuje mnoho IAM řešení třetích stran, která mohou obsahovat další přidané vlastnosti a funkce.

Identity as a Service (IDaaS) je novou metodou IAM, nabízenou řadou společností. Poskytovatelé cloudových služeb mají vlastní IAM řešení: Azure Active Directory, AWS IAM a Goodle Cloud IAM kontrolují přístup ke cloudovým službám, ale organizace s cloudovými i on-premises zdroji mohou využívat vícero rozdílných IAM řešení dohromady.

Pro účely souladu s GDPR je kontrola identit a přístupů využita k omezování přístupu k osobním údajům a k nastolování principu minimálních práv (principle of least privilege), aby měli přístup pouze ti, kteří jej potřebují.

Síťová bezpečnost a prevence narušení bezpečnosti údajů



Síťová bezpečnost pokrývá širokou škálu technologií a je v srdci všech strategií určených k ochraně a k zabezpečení osobních údajů. Zahrnuje prevenci neautorizovaného přístupu pomocí vzdáleného útoku i efektivní řízení aktualizace, posuzování zranitelnosti, firewally, izolaci sítě, multifaktorovou autentizaci pro log-on do sítě a další.

Řešení jako GFI LanGuard a GFI OneGuard mohou vylepšit schopnosti organizace detekovat zranitelnosti v síti ještě předtím, než mohou být zneužity a aplikovat odpovídající opravy a napomoci tak ochraně před narušením bezpečnosti údajů a zároveň ochraně před viry v reálném čase. Síťové firewally a brány další generace se schopností odhalení a prevence průniku (IPS z Intrusion Detection and Prevention System), jako je Kerio Control, zase pomáhají poskytovat komplexní opatření síťové bezpečnosti, která udrží útočníky od osobních údajů ve vaší síti.

Webový prohlížeč je oblíbeným vektorem útoku pro malware a pro narušení bezpečnosti údajů, pročež je důležité zajistit, aby tyto útoky únikem osobních údajů nekončily. Existuje mnoho možností, jak zabezpečit činnosti a transakce na síti, včetně správně nakonfigurovaného nastavení v prohlížeči. Řešení, která monitorují stahování z internetu za účelem odhalení zákeřného software, jako je GFI WebMonitor, mohou hrát při ochraně osobních údajů důležitou roli.

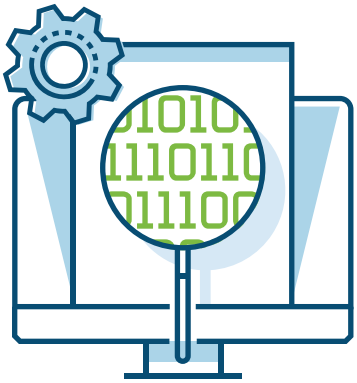
GFI Software™

Emailové zabezpečení

Osobní údaje jsou často posílány emailem, ochrana emailové komunikace je proto životně důležitou součástí dodržování pravidel GDPR. Nasazení řešení pro emailové zabezpečení typu GFI MailEssentials může poskytnout ochranu na více úrovních: skenuje emaily za účelem odhalení virů a malware a zároveň dovoluje nastavit a vynucovat zásady pro obsah, čímž chrání uživatele před záměrným nebo neúmyslným únikem osobních údajů.

Bezpečnostní monitoring a reakce na incidenty

Sledování za účelem odhalení indikátorů bezpečnostních průniků a incidentů je součástí požadavků GDPR – a na trhu je dostupná řada řešení. Operační systém Windows Server sice poskytuje záznamy o bezpečnostních událostech, ale bez dedikovaného řešení, které by dokázalo snadno rozpoznat podezřelou aktivitu v reálném čase, abyste mohli zareagovat co nejrychleji, může být hledání v záznamech složité. Microsoft Azure Security Center může pomoci s monitoringem bezpečnostních událostí a s nastavením upozornění k detekci hrozeb v cloudu.



Zatímco prevence a mitigace narušení bezpečnosti údajů jsou nejvyšší prioritou, dokumentace je také zásadní, když jde o soulad s GDPR; musíte být nejen schopni reagovat – musíte být také schopni později přesně prokázat, kdy a jak jste reagovali.

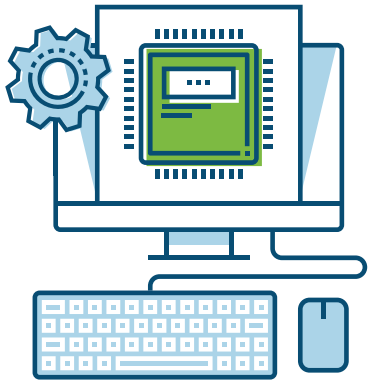
Řešení pro správu událostí typu GFI EventsManager vám dodá jasnější přehled o bezpečnosti týkajících se zásadách, mechanismech, činnostech a aplikacích pro možnost rychlejší reakce na incidenty a umožňuje třívrstvou konsolidaci dat ze záznamů pro oznamování autoritám v souladu s nařízením, navíc chráněné dvoufaktorovou autentizací. Tyto informace mohou být nápomocné také při přípravě DPIA.

Kontrolní záznamy a oznamování

Provádění auditů sítí je součástí testování, posuzování a hodnocení efektivnosti vašich opatření síťové bezpečnosti a je jedním z konkrétních požadavků GDPR. Nástroje pro audit jsou dostupné v operačních systémech i v cloudových službách, ale i v této oblasti vám mohou řešení třetích stran pomoci vylepšit vaše schopnosti dodržovat požadavky GDPR.

Výše zmiňovaný GFI LanGuard nabízí centralizované analýzy a provádění auditů vaší sítě, které zahrnují aplikace a nastavení, jež mohou být bezpečnostními riziky. Umožňuje vám prohlížet si stav bezpečnostních aplikací, otevřených portů, oddílů sdílených souborů, nepotřebných služeb běžících na vašich počítačích a vidět zařízení a aplikace ve vaší síti – všechno co může mít dopad na úroveň ochrany, která je poskytována osobním údajům ve vaší síti.

Hardwarová řešení



Nasazení kombinovaných řešení pro síťový přístup, zabezpečení před viry, malware, k odhalování a prevenci průniků, správu VPN a filtrování webového obsahu může být drahé, nárazově při zřizování i dlouhodobě, kdy se takovýto postup může jednoduše proměnit v masivní administrativní náklady. Především malé společnosti s těsným rozpočtem mohou najít přínos v nasazení „vše v jednom“ Unified Threat Management (UTM) zařízení, která slouží jako firewall, router, IPS, AV, anti-malware, brána VPN a filtr webu a aplikací.

Série UTM zařízení Kerio Control NG poskytuje ochranu, která pomáhá splňovat bezpečnostní požadavky GDPR a zároveň vytváří hlášení, která mohou být prospěšná k dokumentaci zavedených opatření pro soulad s GDPR.

Centralizované řízení přes web se vzdálenou administrativou zjednodušuje sledování a řízení více jednotek Kerio Control . Zařízení jsou kompatibilní s vaším již existujícím prostředím, podporují autentizaci Microsoft Active Directory a Apple Open Directory i autentizaci místní uživatelské databáze a dvou stupňovou verifikaci při vzdáleném přístupu pro lepší bezpečnost.

Shrnutí

Splnění nových nařízení o ochraně dat, která vejdou v platnost v květnu 2018, je náročným a komplikovaným úkolem. Nicméně pro organizace, které sbírají, kontrolují a zpracovávají osobní údaje občanů EU je splnění těchto nařízení povinností. Čas na vytvoření plánu k identifikaci, klasifikaci, řízení, zabezpečení a dokumentaci ochrany těchto údajů a na implementaci řešení, která splní všechny požadavky GDPR, rychle utíká.

Využitím kombinace standardních protokolů a technologií spolu s funkcemi a funkcionalitami zabudovanými do vašich operačních systémů a zahrnutých cloudovými poskytovateli ve vašich cloudových službách zároveň s řešeními třetích stran, jako těch nabízených společnostmi GFI a Kerio, můžete jednoduše implementovat opatření, která vám ke splnění všech požadavků GDPR pomohou ještě před rychle se blížícím vstupem nařízení v platnost.

EUROPE, MIDDLE EAST AND AFRICA

Mooslackengasse 17, Wien, 1190, Austria
Telephone: +43 (1) 928 7374
Fax: +43 (1) 25 3033 30035
sales@gfi.com

ZEBRA SYSTEMS s.r.o.

Výhradní zastoupení GFI Software pro Českou republiku a Slovensko
Opavská 6230/29a,708 00 Ostrava-Poruba, telefon: +420 596 912 961
info@zebra.cz

Pro úplný seznam kanceláří/kontaktů GFI, prosíme, navštivte http://www.gfi.com/contactus

GFI Software™

Pokud jste v dokumentu objevili jakékoli faktické chyby, kontaktujte nás prosím. Revize dokumentu bude provedena, jakmile to bude možné.