Oracle pomáhá organizacím připravit se na nové nařízení EU o Ochraně Osobních Údajů (GDPR)

Dinesh Rajasekharan, Senior Product Manager, Jaroslav Novotný, Architekt, specialista na veřejnou správu, Ivo Fibiger, konzultant, Vít Nohejl, konzultant, Oracle Czech, s.r.o.

Abstrakt

Skutečností posledních let je, že naše osobní data jsou vystavena neustále se zvyšujícímu riziku zneužití díky nárůstu kybernetické kriminality a dalších hrozeb, pocházejících ze světa ICT. Proto má velký smysl snaha Evropské Unie zavést taková opatření, která by tato rizika eliminovala nebo minimalizovala.

Ohledně nařízení EU o Ochraně Osobních Údajů (GDPR) stále panuje spousta nejasností a obecné vnímání je, že se jedná o složitou problematiku.

Nařízení GDPR je bezpochyby velmi užitečné, protože definuje jednotný bezpečnostní rámec a přesná pravidla jeho naplnění. Díky řešením, která poskytuje společnost Oracle je možné účinně a snadno zajistit, že data a informace ve vašich informačních systémech budou tuto normu z velké části naplňovat. Budou tak zabezpečeny nejen z hlediska této normy, ale i z hlediska dalších (často i přísnějších) interních bezpečnostních směrnic, které mohou ve vašich organizacích zavedeny.

V tomto článku popíšeme základní principy a pravidla normy GDPR ve zjednodušené formě. Zaměříme se na to, jak je možné prostředky a řešeními, které poskytuje společnost Oracle, tuto normu naplnit.

Základní informace o GDPR

Snaha o standardizaci ochrany dat byla v rámci Evropské Unie poprvé realizována před více než dvaceti lety formou směrnice o Ochraně Dat 95/46/EC. Tato směrnice však dávala členským státům přílišnou míru volnosti v jejím zavedení do národního práva. Z tohoto důvodu je interpretace této směrnice v různých státech rozdílná. Postupem času se směrnice ukazuje být nedostatečná. Za posledních 20 let se prostředí značně proměnilo a přišly nové výzvy, kterým je potřeba při ochraně dat čelit. Například se značně zvýšil počet útoků na citlivá podniková data, zrychlil se technologický vývoj a zvýšila se míra globalizace. V důsledku těchto, před dvaceti lety těžko předvídatelných skutečností musela Evropská Unie modernizovat právní úpravu ochrany osobních dat. Ve snaze podchytit tuto situaci vyvinula Evropská Unie Nařízení o Ochraně Osobních Údajů (GDPR).

Klíčové cíle GDPR

Ustanovit ochranu soukromí jako základní lidské právo

Základním lidským právem každého jedince je podle GDPR právo na ochranu dat. Každá instituce se sídlem v EU, nebo každý, kdo nakládá s osobními daty osob z EU, musí mít procesy a technologii nastavenou tak, aby byla osobní data efektivně zabezpečena.

Upřesnit odpovědnost jednotlivých subjektů

GDPR se vztahuje na každého Zpracovatele nebo Správce se sídlem v EU nebo založeného v EU. Dále na subjekty nesídlící v EU, ale poskytující své služby subjektům sídlícím v EU.

Definovat předmět datové ochrany

Pro omezení nejednotnosti a roztříštěnosti právních výkladů zavádí GDPR základní definici datové ochrany, která musí být dodržena každým subjektem zpracovávajícím osobní data subjektů z EU.

Rozšířit možnosti datové ochrany

GDPR pokládá šifrování pouze za jednu z mnoha komponent bezpečnostní strategie. Je stanoveno, že organizace musí zavést a vyhodnocovat pravidelné kontroly na základě úrovně citlivosti daných osobních dat.

Zvýšit vymahatelnost práva

EU podmiňuje dodržování směrnice GDPR hrozbou vysokých pokut a to až do výše 4% globálního ročního příjmu.

Klíčové subjekty v GDPR

GDPR definuje řadu nových termínů, pomocí kterých vysvětluje bezpečnostní koncepty a s nimi sdružené role.

Subjekty údajů jsou lidé, kteří mohou být z dat buď přímo, nebo nepřímo identifikováni. Identifikátor může být například číslo kreditní karty, uživatelské jméno, nebo webový cookie.

Osobní data jsou jakékoliv osobní informace, včetně citlivých dat, vztahující se k danému subjektu. Například adresa, den narození, jméno nebo národnost.

Správce je fyzická nebo právnická osoba, veřejný či jiný subjekt, který samostatně nebo společně s dalšími subjekty rozhoduje o důvodech a způsobech zpracování osobních dat. Správcem může být například firma nebo CIO (Chief Information Officer).

Pověřenec pro ochranu osobních údajů (DPO, Data Protection Officer) je jedinec pracující pro Správce nebo Zpracovatele s rozsáhlými znalostmi o datovém soukromí a standardech datové bezpečnosti. DPO radí Správci a Zpracovateli s jejich povinnostmi v souladu s GDPR a hlídá správnou implementaci. DPO funguje jako zprostředkovatel mezi Správcem / Zpracovatelem a Dohlížejícím subjektem. DPO může být například Chief Security Officer nebo Bezpečnostní Administrátor.

Zpracovatel je fyzická nebo právnická osoba, veřejný či jiný subjekt zpracovávající osobní data na požadavek Správce. Například vývojář, tester nebo analytik.

Příjemce je fyzická nebo právnická osoba, veřejný či jiný subjekt, kterému jsou osobní data poskytnuta. Například jedinec, daňový poradce, pojišťovací agent nebo agentura.

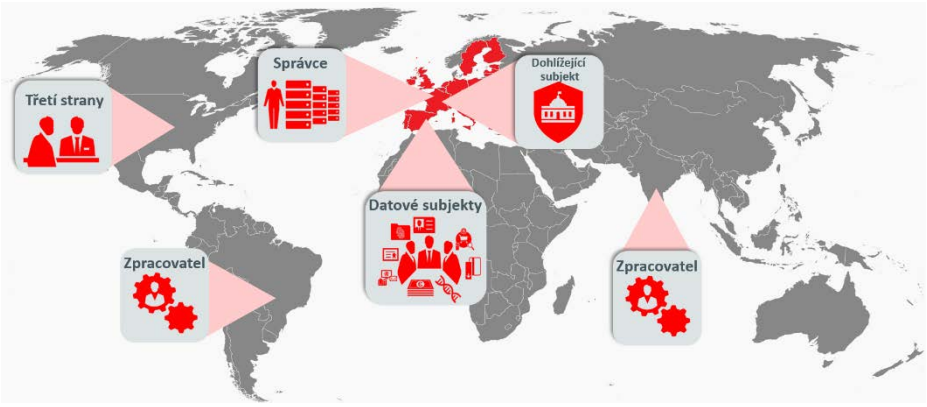
Podnik je jakákoliv právnická nebo fyzická osoba provozující ekonomickou aktivitu. To v zásadě zahrnuje všechny organizace jak v soukromém, tak veřejném sektoru ať už pocházející z EU, nebo odjinud.

Třetí strana je fyzická nebo právnická osoba, veřejný či jiný subjekt, který není Datovým Subjektem, Správcem, Zpracovatelem, a která má z pověření Správce nebo Zpracovatele oprávnění zpracovávat data. Například partneři nebo kontraktoři.

Dohlížející subjekt je nezávislá veřejná autorita založená členským státem (také známá jako Národní autorita datové bezpečnosti pod současnou směrnicí EU o ochraně dat) nebo auditující společnost.

Hypotetický příklad

Pro lepší porozumění jednotlivým termínům, jejich rolím a vztahům zde uvedeme příklad hypotetické výrobní společnosti XYZ sídlící ve Francii. Zákazníci společnosti XYZ objednávají výrobky online přes webový portál. V souladu se svým obchodním modelem si společnost XYZ ukládá a zpracovává data o jednotlivcích (**Subjektech údajů**). Tato společnost se sídlem v EU rozhoduje o důvodech a způsobech zpracování osobních údajů (**Správce**). Vývoj, testování, péče o zákazníky a účetnictví je outsourcováno externím dodavatelům z Brazílie a Indie (**Zpracovatel**). V těchto subjektech si zaměstnanci často kopírují osobní data do svých lokálních vývojářských a testovacích systémů. XYZ má také uzavřené partnerství s platebními a doručovacími společnostmi (**Třetí strany**) z různých zemí. Těmto společnostem poskytuje XYZ data (**Osobní data**) potřebná k vyřízení objednávek. Nezávislý veřejný subjekt monitoruje soulad s GDPR (**Dohlížející subjekt**). Následující obrázek zobrazuje ukázku geografické distribuce výše zmíněných subjektů.



Hlavní bezpečnostní požadavky

Hlavní bezpečnostní požadavky, které přináší GDPR můžeme rozdělit do třech kategorií: posouzení vlivu, prevence a monitorování. Zjednodušeně řečeno GDPR vyžaduje dodržování bezpečnostních zásad s cílem zvýšit kvalitu ochrany dat. Následující odstavce shrnují klíčové požadavky na zabezpečení dat dle GDPR.

Posouzení vlivu bezpečnostních rizik

GDPR požaduje, aby Správce dat prováděl tzv. posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment). Tento proces má pomoci odhalit místa, která mohou představovat „vysoké riziko“ úniku dat. Posouzení musí obsahovat hloubkové hodnocení procesů organizace. Cílem je zjistit, jaký mají tyto procesy dopad na ochranu osobních dat a zda vyhovují požadavkům na ochranu dat. Výsledky tohoto „auditu“ slouží jako základ efektivní prevence proti útokům.

Prevence proti útokům

Prevence narušení bezpečnosti je v nařízení GDPR často zmiňovaným termínem. V nařízení je doporučeno několik technik, jak se před útoky preventivně bránit.

Šifrování

Dle GDPR je šifrování jednou z klíčových technik zajištění nesrozumitelnosti dat neoprávněným uživatelům. Pro zajímavost GDPR stanovuje, že v případě úniku dat není Správce povinen informovat Subjekty údajů, pokud jsou data šifrována a tudíž jsou pro útočníka nečitelná.

Anonymizace a Pseudonymizace

Datová anonymizace je technika, pomocí které jsou data zakódována a maskována. Tím pádem data nemohou být použita v identifikaci určitého člověka a nejsou s ním nijak spojitelná.

Pseudonymizace slouží k omezení spojitosti mezi daty a identitou Subjektu údajů.

Vedení záznamů o činnostech oprávněných uživatelů

GDPR navrhuje zavedení kontrol oprávněných uživatelů, kteří mají k přístup k osobním datům. Tím se zabrání útokům zevnitř nebo ze zpronevěřených účtů.

Přístupová práva s vysokou granularitou

Kromě kontroly oprávněných uživatelů navrhuje GDPR také zavedení přístupových práv s vysokou granularitou. Tím se zajistí, že k datům je přistupováno pouze z konkrétních a předem definovaných důvodů.

Omezit nakládání s osobními údaji na minimum

GDPR doporučuje minimalizovat sběr a dobu uchovávání Osobních údajů. Při sběru, zpracovávání a sdílení Osobních údajů musí být Správci a Zpracovatelé obezřetní a omezit množství informací na minimum nutné pro danou aktivitu.

Monitoring jako zbraň pro včasné odhalení hrozby

Preventivní bezpečnostní opatření pomáhají minimalizovat riziko útoku. Nemohou však zcela vyloučit, že se případná narušení bezpečnosti objeví. GDPR doporučuje monitorování a systém včasného varování jako účinnou zbraň proti narušení bezpečnosti. Pomoci mohou především tyto mechanismy:

Datový audit

GDPR nařizuje nejen nahrávání a audit činností týkajících se osobních dat, ale také nařizuje Správci uchovávat tyto záznamy. Jinými slovy tyto záznamy musejí být zabezpečeny proti manipulaci či smazání. Třetí strany či Zpracovatelé k těmto záznamům nesmějí mít přístup. Datový audit pomáhá odhalit, zda jsou činnosti týkající se monitoringu správně nastaveny.

Monitoring a včasné varování

GDPR nařizuje neustálý monitoring a zavedení systému včasných varování. Tyto mechanismy jsou rozhodující pro detekci anomálií.

Existují tak tři hlavní kategorie směrnic, které pomáhají organizaci řešit hrozící nebezpečí. Těmito kategoriemi jsou posouzení vlivu bezpečnostních rizik, prevence proti útokům a detekce anomálií.

Kvalita ochrany dat

V minulosti organizace nebyly povinné zajistit kvalitní ochranu dat a vše fungovalo na dobrovolné bázi. GDPR je směrnicí nařizující bezpečnostní standardy malým i velkým subjektům. Díky GDPR je zaručena stejná kvalita ochrany dat napříč všemi organizacemi i odvětvími.

Centralizace

GDPR doporučuje zajišťovat bezpečnost dat centralizovaně. Takovéto řešení vede při správě více aplikací či systémů k včasným opatřením v případě hrozících či odhalených hrozeb. Dalším požadavkem je centralizace kontrol. Ty pomáhají díky jednotným bezpečnostním požadavkům a cílům zvýšit pravděpodobnost odhalení bezpečnostní hrozby. Navíc dochází k používání osvědčených praktik a postupů napříč organizací.

Komplexní zabezpečení

Organizace musí být připravena na útoky z různých zdrojů. GDPR nařizuje komplexní ochranu osobních dat ve všech fázích životního cyklu dat. Ať už se jedná o data uložená, dlouho nepoužívaná či data se kterými se právě pracuje.

GDPR a databáze Oracle

Společnosti mají typicky několik vrstev zabezpečení, které chrání jejich databáze. Je to např. firewall, systém na detekci útoku, segmentace sítě apod. Všechny tyto systémy brání útočníkům přistoupit k datům. S rozvojem technologií se však tradiční hranice rozplývají a stále více lidí má přímý přístup k databázi (administrátoři, testeři, vývojáři, partneři). Důkladné zabezpečení je tedy zcela nezbytné. Ve snaze zmenšit prostor, který by útočníci mohli napadnout, a snížit tak množství způsobů, jak by mohli získat přístup do databáze, je extrémně důležité nasadit zabezpečení co nejblíže k samotným datům.

Jedním z úkolů při zkoumání bezpečnostních rizik je zjistit, co je potřeba vyhodnotit. Databázové aplikace totiž typicky obsahují několik vstupních bodů ze sítí, operačních systémů, databází a i ze samotných aplikací.

Útočníci mohou využít slabinu v jakémkoliv vstupním bodu. Navíc se mohou zaměřit i na samotné zaměstnance a partnery, kteří jsou odpovědní za užívání, správu, testování a udržování systému.

Vyhodnocení bezpečnostních rizik

GDPR vyžaduje vyhodnotit dopady datového zabezpečení pro určité typy datového zpracování. Hlavní výzvou při vyhodnocování bezpečnostních rizik je rozhodnutí, co vůbec vyhodnocovat. Dnešní databázové aplikace typicky obsahují několik vstupních bodů a osobní data jsou v nich rozprostřena přes mnoho sloupců a tabulek. Situaci komplikují také často volně definovaná přístupová oprávnění.

Technologie a produkty databázového zabezpečení Oracle poskytují nástroje pro vyhodnocení mnoha aspektů dat aplikace:

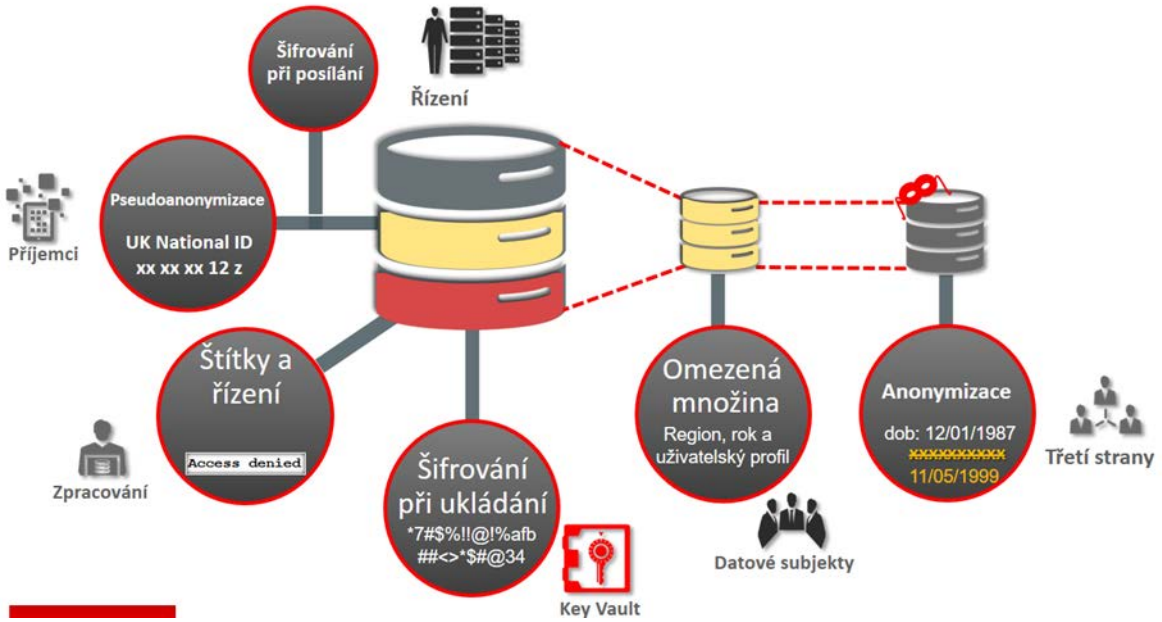
- Určení tabulek a sloupců obsahující Osobní data
- Konfigurace databází a zjištění celkového bezpečnostního profilu
- Analýza databázových rolí a oprávnění
- Analýza, jakým způsobem přistupují k osobním datům správci, zpracovatelé, třetí strany, datové subjekty a příjemců

Prevence proti útokům II

Výše byla zmíněna preventivní opatření a techniky, které GDPR doporučuje. Jednalo se např. o šifrování, pseudonymizaci, anonymizaci, kontrolu přístupu oprávněných uživatelů apod. Skutečnou výzvou zůstává samotné zavedení těchto vrstev preventivní datové ochrany. V mnoha případech mohou způsobit značné navýšení režijních nákladů nebo komplikaci každodenních IT operací. Komplikace se mohou projevit v podobě změny procesů, změn ve zdrojovém kódu aplikace, testování, snížení výkonu či problémů spojených se škálovatelností. Vzhledem k těmto výzvám mohou některé společnosti se zavedením preventivních opatření do již existujících aplikací váhat.

Drtivou většinu těchto komplikací řeší zabezpečení Oracle Database, které má minimální dopad na výkon a na každodenní IT operace. Oracle nabízí jednoduše implementovatelnou sadu nástrojů, která pomáhá se zavedením preventivních kontrol navrhovaných v GDPR. Např.:

- Šifrování uložených dat za pomoci Transparent Data Encryption
- Centrální správa šifrovacích klíčů pomocí Oracle Key Vault
- Šifrování přenášených dat pomocí Oracle Database Network Encryption a Data Integrity
- Pseudonymizace dat pomocí Data Redaction a Database Vault
- Anonymizace a minimalizace za použití Oracle Data Masking a Subsetting
- Záznamy o uživatelích a rozdělení povinností a oprávnění pro každého uživatele za pomocí Oracle Database Vault
- Selektivní skrytí dat za pomoci Oracle Virtual Private Database
- Kontrola přístupů s Oracle Label Security
- Kontrola přístupů koncových uživatelů s pomocí Oracle Real Application Security

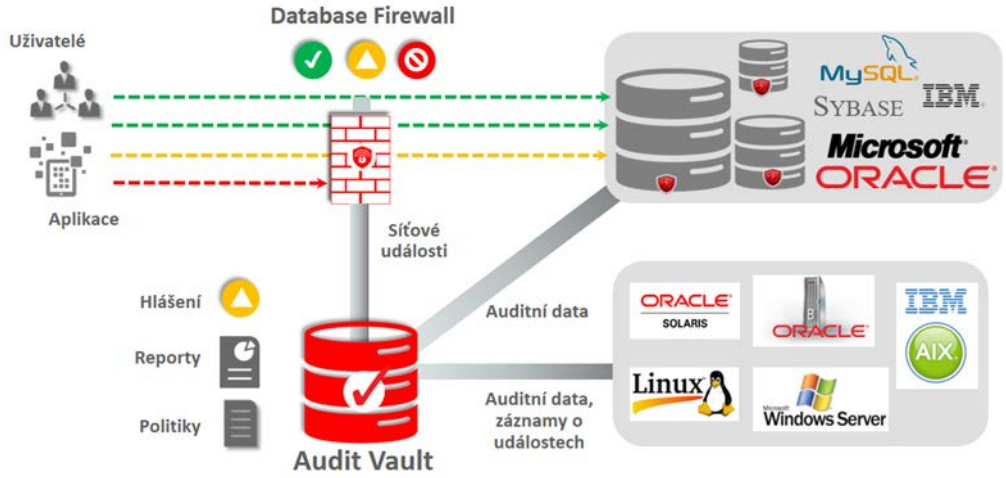


Monitoring jako zbraň pro včasné odhalení hrozby

Tradiční firewally hrají důležitou roli při ochraně datových center před neoprávněnými přístupy. Nicméně útoky jsou stále efektivnější a sofistikovaně obcházejí bezpečnostní opatření. Statistiky o bezpečnostních incidentech ukazují, že včasné prozkoumání výsledků datového auditu může pomoci odhalit neoprávněné aktivity včas a snížit riziko potenciálních finančních dopadů. GDPR stanovuje, že organizace musí ukládat záznamy o svých činnostech týkajících se osobních dat. Toho lze dosáhnout pouze konstantním monitoringem a pravidelnými datovými audity. Získaná data pak slouží jako základ pro vytvoření systému včasného varování. Centralizovaná kontrola brání útočníkům či uživatelům se zlými úmysly zahladit stopy své podezřelé aktivity.

POSOUDIT	OCHRÁNIT	ODHALIT
Procesy, Profily, Citlivost dat, Rizika	Šifrování, Pseudonymizaci, Anonymizace, Detailní řízení přístupu, Řízení privilegovaných přístupů, Oddělení rolí	Audit, Monitorování aktivit, Upozorňování, Reportování

Oracle Database Security poskytuje komplexní nástroje pro audit a systémy pro reporting tak, aby byly splněny požadavky GDPR. Oracle Audit Vault a Database Firewall (AVDF) nabízí možnost datového auditu a ochranou (DCAP) platformu nové generace. Ta poskytuje komplexní a flexibilní monitorování prostřednictvím konsolidace auditovaných dat z Oracle i jiných databází, operačních systémů, souborových systémů a dat z konkrétních aplikací. Současně Oracle Database Firewall může působit jako první linie ochrany v datové síti, která pomáhá odhalit škodlivou činnost nad databázemi.



Shrnutí

GDPR přináší řadu nařízení a regulací v oblasti datové bezpečnosti. Reakci je nezbytné začít včas plánovat. Společnost Oracle je už po desítky let v oblasti datové bezpečnosti nesporně na špici, co se týče šíře a kvality portfolia řešení, které nabízí. Sada produktů Oracle Database Security nabízí vysokou míru transparence, minimální navýšení nákladů a snadné zavedení. Produkty Oracle Database umožňují organizacím rychlé zavedení bezpečnostních požadavků GDPR a především dosáhnout silného zabezpečení pro osobní a podniková data.