GDPR

Všeobecné nariadenie o ochrane osobných údajov

4. mája 2016 bolo v Úradnom vestníku Európskej únie zverejnené nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „nariadenie"). Organizácie sú povinné sa zosúladiť s požiadavkami tohto nariadenia do **25. mája 2018**, odkedy začne byť nariadenie účinné.

ZMENY A NOVÉ POŽIADAVKY

POKUTA AŽ 20 000 000€
alebo 4% z ročných tržieb spoločnosti/organizácie

ÚČINNOSŤ OD 25. 05. 2018

Problém

Zavedenie nového nariadenia vyžaduje zmeny v procesoch i v technológiách. Nedodržanie nariadenia môže viesť k pokute 20 mil. euro alebo 4 % z ročných tržieb spoločnosti/organizácie. Účinnosť – od 25. 5. 2018.

Koho sa týka?

Spracúvate údaje o klientoch? Máte zamestnancov, prístupový, kamerový systém alebo e-shop? Využívate dáta na marketingové účely? Ak ste aspoň na jednu otázku odpovedali áno, **GDPR sa vás týka**.

Riešenie

Znížime vaše bezpečnostné riziká a zoptimalizujeme náklady. Analyzujeme rozdiely voči nariadeniu GDPR, navrhneme opatrenia i procesy, nasadíme technológie a zabezpečíme ich prevádzku.

www.tempest.sk/GDPR

Tempest
IT makes sense

Nakoľko novoprijatá regulácia môže mať praktický dopad aj na Vašu organizáciu, ponúkame Vám spoluprácu pri riešení implementácie požiadaviek týkajúcich sa tejto oblasti. Súčasne v tabuľke nižšie sú v prehľadnej forme uvedené možné dopady nariadenia na organizácie z hľadiska implementácie dodatočných opatrení.

Požiadavky vyplývajúce z GDPR	Ako vám môže TEMPEST pomôcť?
Zabezpečenie primeranej úrovne bezpečnosti informačných systémov, posúdenie rizík súvisiacich so spracúvaním osobných údajov a prijatie primeraných bezpečnostných opatrení.	• Preverenie stavu organizácie a jej pripravenosti na plnenie požiadaviek nariadenia (analýza súladu organizácie s nariadením) a návrh opatrení na zosúladenie organizácie s požiadavkami nariadenia. • Podpora pri zosúlaďovaní organizácie s požiadavkami nariadenia. • Vypracovanie analýzy rizík/posúdenia vplyvu spracovateľských operácií na ochranu osobných údajov. • Implementácia systémov manažérstva informačnej bezpečnosti a manažérstva IT služieb.
Zavedenie organizačných opatrení.	• Vypracovanie politík/smerníc podporujúcich ochranu osobných údajov v organizácii a ostatnej bezpečnostnej dokumentácie.
Vedenie záznamov o spracovateľských činnostiach.	• Identifikácia informačných systémov osobných údajov a vypracovanie záznamov.
Zabezpečenie zmluvných záruk.	• Podpora pri zosúlaďovaní organizácie v oblasti zabezpečenia zmluvných záruk.
Povinnosť určenia zodpovednej osoby.	• Zabezpečenie podpory pri výkone dohľadu nad ochranou osobných údajov. • Outsourcing osoby zodpovednej za výkon dohľadu nad ochranou osobných údajov.
Prevencia pred únikom dát/osobných údajov.	• Implementácia Data Loss Prevention systémov.
Šifrovanie dát/osobných údajov.	• Implementácia EndPoint Security nástrojov na ochranu pracovných staníc a na šifrovanie údajov na pracovných staniciach, serveroch a pri ich prenose. • Implementácia nástrojov na ochranu mobilných zariadení (Mobil Device Management).
Zvyšovanie povedomia zamestnancov v oblasti ochrany osobných údajov.	• Školenia zamerané na ochranu osobných údajov, na požiadavky nariadenia a jeho uplatňovanie v praxi. • Školenia zamerané na zvyšovanie bezpečnostného povedomia.
Predchádzanie neoprávnenému prístupu k osobným údajom.	• Implementácia nástrojov na správu používateľov a riadenie prístupových práv (IDM, PIM, AM, SSO a pod.). • Implementácia nástrojov pre silnú autentifikáciu (smartcards, USB tokeny, Soft tokeny, OTP a pod.).

Požiadavky vyplývajúce z GDPR	Ako vám môže TEMPEST pomôcť?
Pseudonymizácia/anonymizácia osobných údajov.	• Vývoj na základe potrieb zákazníka. • Implementácia podporných nástrojov na pseudonymizáciu/anonymizáciu údajov (napr. Oracle Data Masking Pack).
Zabezpečenie včasnej obnovy osobných údajov.	• Návrh Disaster Recovery plánov (plánov obnovy) a zavedenie procesov riadenia kontinuity činností v organizácii. • Implementácia riešení zálohovania, archivácie a obnovy údajov. Zabezpečenie deduplikácie údajov. • Implementácia riešení vysokej dostupnosti (clustering, disaster recovery). • Návrh a implementácia nástrojov na sledovanie dostupnosti (fault), výkonnosti (performance) a kapacity IKT infraštruktúry.
Zabezpečenie získania a prenosnosti osobných údajov v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte.	• Vývoj na základe potrieb zákazníka.
Zabezpečenie bezpečného mazania/likvidácie osobných údajov.	• Vývoj na základe potrieb zákazníka. • Implementácia EndPoint Security nástrojov na bezpečné mazanie údajov.
Zabezpečenie integrity osobných údajov. Riadenie a monitorovanie aktivít s osobnými údajmi.	• Návrh a implementácia nástrojov na monitoring siete, telekomunikačnej infraštruktúry, operačných systémov, databáz, aplikačných serverov, middlewaru a aplikácií. • Vývoj pre oblasť Big Data/DWH riešení. • Implementácia riešení na efektívnu správu informácií v organizácii (eOffice).
Zabezpečenie odolnosti systémov spracúvania osobných údajov a podporných služieb. Zabezpečenie sieťovej bezpečnosti a ochrany infraštruktúry spracúvajúcej osobné údaje pred internými/externými hrozbami.	• Implementácia systémov detekcie a prevencie prienikov (IDS/IPS). • Zabezpečenie ochrany počítačových sietí (FW) a webových stránok a portálov (WAF). • Implementácia antivírusovej, antispamovej, resp. AntiX ochrany na úrovni internetových brán. • Implementácia Data Loss Prevention (DLP) systémov. • Implementácia databázových firewallov.
Schopnosť včas identifikovať bezpečnostné incidenty, analyzovať ich, zdokumentovať ich a informovať o nich.	• Zavedenie procesov riadenia bezpečnostných incidentov. • Zavedenie podporných nástrojov na evidenciu a riešenie incidentov (napr. HP Service Manager, SIEM).
Pravidelné testovanie bezpečnosti osobných údajov.	• Realizácia bezpečnostných auditov zameraných na identifikáciu úrovne naplnenia požiadaviek nariadenia. • Realizácia penetračných testov a testovanie zraniteľností.

www.tempest.sk/GDPR

Tempest
IT makes sense

Zmeny a požiadavky súvisiace s GDPR

Nariadenie zavádza nové definície pojmov súvisiace s ochranou osobných údajov (ako sú napríklad pseudonymizácia, profilovanie, genetický údaj, skupina podnikov).

Využívané online identifikátory pridelené fyzickým osobám technickými prístrojmi, ako sú **IP adresy, cookies, RFID, e-mailové adresy, lokalizačné údaje** a pod. môžu byť za istých okolností chápané ako osobné údaje.

Upravuje podmienky spracúvania osobných údajov v súvislosti s ponukou služieb informačnej spoločnosti

Upravuje **podmienky automatizovaného rozhodovania vrátane profilovania**, pri ktorom má dotknutá osoba právo namietať voči rozhodnutiu, ktoré je založené na takomto automatizovanom rozhodovaní.

Upravuje osobitnú ochranu osobných údajov vzťahujúcu sa na **využívanie osobných údajov detí** s dopadom na povinnosti prevádzkovateľov informačných systémov osobných údajov.

Upravuje podmienky vzájomných zmluvných vzťahov (**vyžaduje úpravu aj už existujúcich zmluvných vzťahov**):

- medzi viacerými prevádzkovateľmi toho istého informačného systému osobných údajov,
- medzi prevádzkovateľom a sprostredkovateľom,
- medzi sprostredkovateľom a jeho ďalším sprostredkovateľom.

Rozširuje povinnosti prevádzkovateľov vo vzťahu k informačnej a oznamovacej povinnosti voči dotknutým osobám.

Ustanovuje **povinnosť prijatia primeraných technických a organizačných opatrení**, ako sú napríklad pseudonymizácia, šifrovanie, schopnosť včas obnoviť dostupnosť údajov, zavedenie politík a smerníc. Súčasne ustanovuje **povinnosť posúdenia primeranej úrovne bezpečnosti** s prihliadnutím na riziká, ktoré samotné spracúvanie predstavuje.

Zmeny a požiadavky súvisiace s GDPR

Rozširuje povinnosti a zodpovednosti sprostredkovateľov vo vzťahu k spracúvaniu osobných údajov.

Ustanovuje **povinnosť vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov**. V závislosti od výsledkov posúdenia vplyvu na ochranu údajov zavádza povinnosť konzultácie s dozorným orgánom pred začatím spracúvania.

Ustanovuje **oznamovaciu povinnosť o porušení ochrany osobných údajov** voči dozornému orgánu (najneskôr do 72 hodín) a voči dotknutej osobe.

Zavádza, v nariadením určených prípadoch, povinnosť určenia zodpovednej osoby, a to pre prevádzkovateľa aj sprostredkovateľa. Súčasne upravuje aj povinnosti a právomoci zodpovednej osoby.

Zavádza **právo dotknutej osoby na prenosnosť údajov** od jedného prevádzkovateľa druhému prevádzkovateľovi.

Upravuje právo dotknutej osoby, **aby bola informovaná o všetkých osobných údajoch** spracúvaných o svojej osobe u prevádzkovateľa.

Upravuje právo dotknutej osoby na **opravu nesprávnych osobných údajov** alebo na obmedzenie ich spracúvania.

Zavádza právo dotknutej osoby na vymazanie jej osobných údajov („**právo na zabudnutie**"), a to aj tých, ktoré boli získané v súvislosti s ponukou služieb informačnej spoločnosti.

Významne zvyšuje výšky sankcií za neplnenie požiadaviek nariadenia, a to až do výšky **20 000 000 € alebo v prípade podniku až do výšky 4 % z ročných tržieb spoločnosti/organizácie** za predchádzajúci účtovný rok v prípadoch, keď dôjde k porušeniu nariadením stanovených povinností.

TEMPEST a.s.

Galvaniho 17/B
821 04 Bratislava 2
Slovenská republika

informácie a otázky: info@tempest.sk
obchodné záležitosti: obchod@tempest.sk
Tel: +421 (2) 502 67 111