Tempest
IT makes sense

GDPR – dlhá a kľukatá cesta k dosiahnutiu súladu?

Miroslav Fridrich
Branislav Mitas

28.9.2017
Bratislava

OBSAH

Tempest
IT makes sense

- Úvod do GDPR
- Základné piliere GDPR
- Zmeny, ktoré GDPR prinieslo
- Osvedčený prístup riešenia súladu s GDPR
- GDPR a bezpečnostné štandardy
- GDPR a ostatná legislatíva
- Ako zostaviť správny tím
- Najväčšie problémy a výzvy pri riešení GDPR

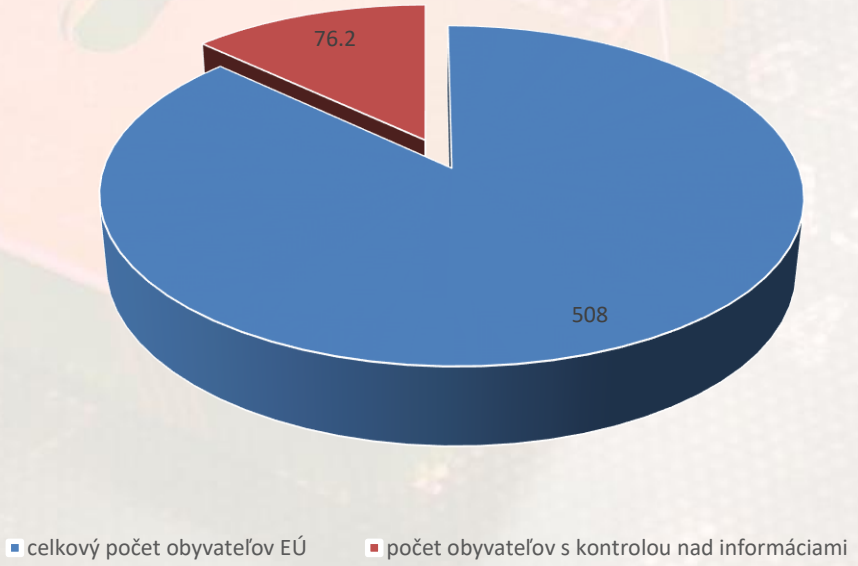
GDPR, ČO TO JE?

Tempest
IT makes sense

- GDPR je skratka Európskeho Nariadenia **General Data Protection Regulation** (2016/679).
- Nový predpis, ktorý je evolúciou v oblasti ochrany osobných údajov.
- Priamo vykonateľné vo všetkých členských štátoch EÚ.
- Účinnosť (uplatňuje sa) od 25 mája 2018.

PREČO GDPR?

- Unifikácia pravidiel na ochranu osobných údajov v EÚ priestore.
- 508 miliónov obyvateľov EÚ, iba 15 % osôb má pocit, že má úplnú kontrolu nad informáciami, ktoré poskytuje online (zdroj: Európska únia, 2017)
- Jednotná úprava ochrany súkromia v EÚ alebo 28 národných pravidiel?
  - Fikcia?



KOHO SA GDPR TÝKA?

Tempest
IT makes sense

- Každý jednotlivec, podnikateľ, firma, organizácia spracúvajúca osobné údaje.

- Približne 579 000 ekonomických subjektov na Slovensku (zdroj: Správa o stave podnikateľského prostredia v SR - Štatistický úrad SR dostupné na http://www.statistics.sk/pls/elisw/vbd).

- Nevzťahuje sa na osobné údaje zosnulých osôb a osobné údaje spracúvané fyzickou osobou výhradne v rámci osobnej alebo domácej činnosti.

ČO JE OSOBNÝ ÚDAJ?

Tempest
IT makes sense

- Meno, priezvisko, adresa
- Dátum narodenia
- Rodné číslo
- Fotografia
- Údaje o zdraví...

- Lokalizačné údaje
- IP adresa
- EČV

- Akékoľvek údaje týkajúce sa konkrétnej FO

5 ZÁKLADNÝCH PILIEROV GDPR

Tempest
IT makes sense

- Obmedziť spracúvanie osobných údajov na stanovené účely.
- Obmedziť uchovávanie osobných údajov.
- Obmedziť rozsah spracúvaných osobných údajov.
- Vyžadovať transparentnosť pri spracúvaní osobných údajov.
- Zaistiť bezpečnosť osobných údajov.

ZMENY PODĽA GDPR KOMPLIKÁCIA/VÝHODA?

Tempest
IT makes sense

- Výkon dohľadu nad ochranou osobných údajov (zodpovedná osoba).

- Prehodnotiť právny základ spracúvania OÚ pre niektoré IS OÚ:
  - návštevný systém (súčasnosť - limitovaný rozsah údajov),
  - kamerové systémy (súčasnosť- verejné priestory, neverejné priestory),
  - ...

ČO GDPR OVPLYVŇUJE?

Tempest
IT makes sense

ĽUDIA

dopad na zamestnancov

definuje nové zodpovednosti

poverenie zodpovednej osoby

vyžaduje vzdelávanie a zvyšovanie bezp. povedomia

PROCESY

dopad na obchodné i technologické procesy

vyžaduje vyššiu kontrolu nad spracúvaním osobných údajov

vyžaduje zavedenie organizačných a zmluvných opatrení

TECHNOLÓGIE

dopad na IT infraštruktúru

ochrana údajov by design vs. by default

zvyšuje nároky na ochranu koncových staníc, serverov, sietí, úložísk, aplikácií, ...

vyžaduje zavedenie technolog. opatrení

DÁTA

mení prístup k bezpečnosti osobných údajov

primeraná úroveň ochrany osobných údajov

schopnosť zabezpečiť trvalú dôvernosť, dostupnosť a integritu

dôraz na kontrolné mechanizmy

PDCA CYKLUS VS. GDPR

Tempest
IT makes sense

- Príprava
  - analýza a pochopenie existujúcich rizík
- Prevencia
  - implementácia opatrení
- Detekcia
  - identifikácia problému/incidentu
- Reakcia a náprava
  - reakcia na problém/incident
  - minimalizácia dopadov

- Príprava a prevencia -> risk management
- Detekcia, reakcia a náprava -> incident management

AKO UCHOPIŤ IMPLEMENTÁCIU GDPR VS. OSVEDČENÝ PRÍSTUP

Tempest
IT makes sense

- analyzovať spracúvané osobné údaje a toky týchto údajov + životný cyklus údajov
  - účely spracúvania, právne základy, rozsah spracúvaných údajov, dotknuté osoby, ostatné subjekty, ktorých sa spracúvanie oú týka
  - identifikovať oprávnené osoby a rozsah ich oprávnení
- posúdiť aktuálny stav plnenia požiadaviek GDPR
- posúdiť riziká súvisiace so spracúvaním osobných údajov
- posúdiť vplyv spracovateľských operácií na ochranu osobných údajov (ak je potrebné)
- identifikovať/nastaviť primeranú úroveň bezpečnosti
- zaviesť nevyhnutné zmeny, ktoré vyžaduje GDPR
  - organizačné (určiť pravidlá pre spracúvanie oú, ...)
  - technologické

RIZIKOVÁ ANALÝZA – ÁNO ČI NIE?

Tempest
IT makes sense

- Čl. 33 – oznamovanie porušenia ochrany oú dozornému orgánu -> s výnimkou prípadov, kedy nie je pravdepodobné, že **porušenie povedie k riziku pre práva a slobody dotknutých osôb** ...
- Čl. 35 – posúdenie vplyvu spracovateľských operácií -> ak typ spracúvania **povedie k vysokému riziku pre** ...
- Čl. 30 - vedenie záznamov o spracovateľských operáciách -> nie je povinné, pokiaľ menej ako 250 osôb, pokiaľ nie je pravdepodobné, že spracúvanie **povedie k riziku pre práva a slobody dotknutých osôb** ...

- Čl. 24 a 25 – ... prijatie vhodných technických a organizačných opatrení **vzhľadom na riziká** pre práva a slobody dotknutých osôb ...
- Čl.32, ods. 1 - ... primerané technické a organizačné opatrenia **s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku** ...
- Čl. 32, ods. 2 – pri posudzovaní primeranej úrovne bezpečnosti **sa prihliada predovšetkým na riziká**, ktoré predstavuje spracúvanie ...

BEZPEČNOSTNÉ ŠTANDARDY

Tempest
IT makes sense

- **ochrana osobných údajov** vs. Confidentiality (dôvernosť) resp. Privacy (ochrana súkromia) (ISO 27002, ISO 27018, ISO 29100)
- **posúdenie primeranej úrovne bezpečnosti** vs. analýza a ohodnotenie rizík (ISO 3100x, ISO 27001, ISO 27005)
- **zabezpečenie trvalej dôvernosti, dostupnosti, integrity a odolnosti systémov spracúvania a služieb** vs. klasifikácia a ochrana informačných aktív (ISO 27002, NIST)
- **schopnosť včas obnoviť dostupnosť oú a prístup k nim** vs. plánovanie kontinuity činností / DRP a BCP (ISO 27002, ISO 22301)
- **identifikácia a oznámenie porušenia ochrany osobných údajov** vs. security incident management (ISO 27035, ISO 27002)
- **pravidelné testovanie, posudzovanie a hodnotenie účinnosti opatrení** vs. implementácia systémov manažérstva IB (najmä ISMS)

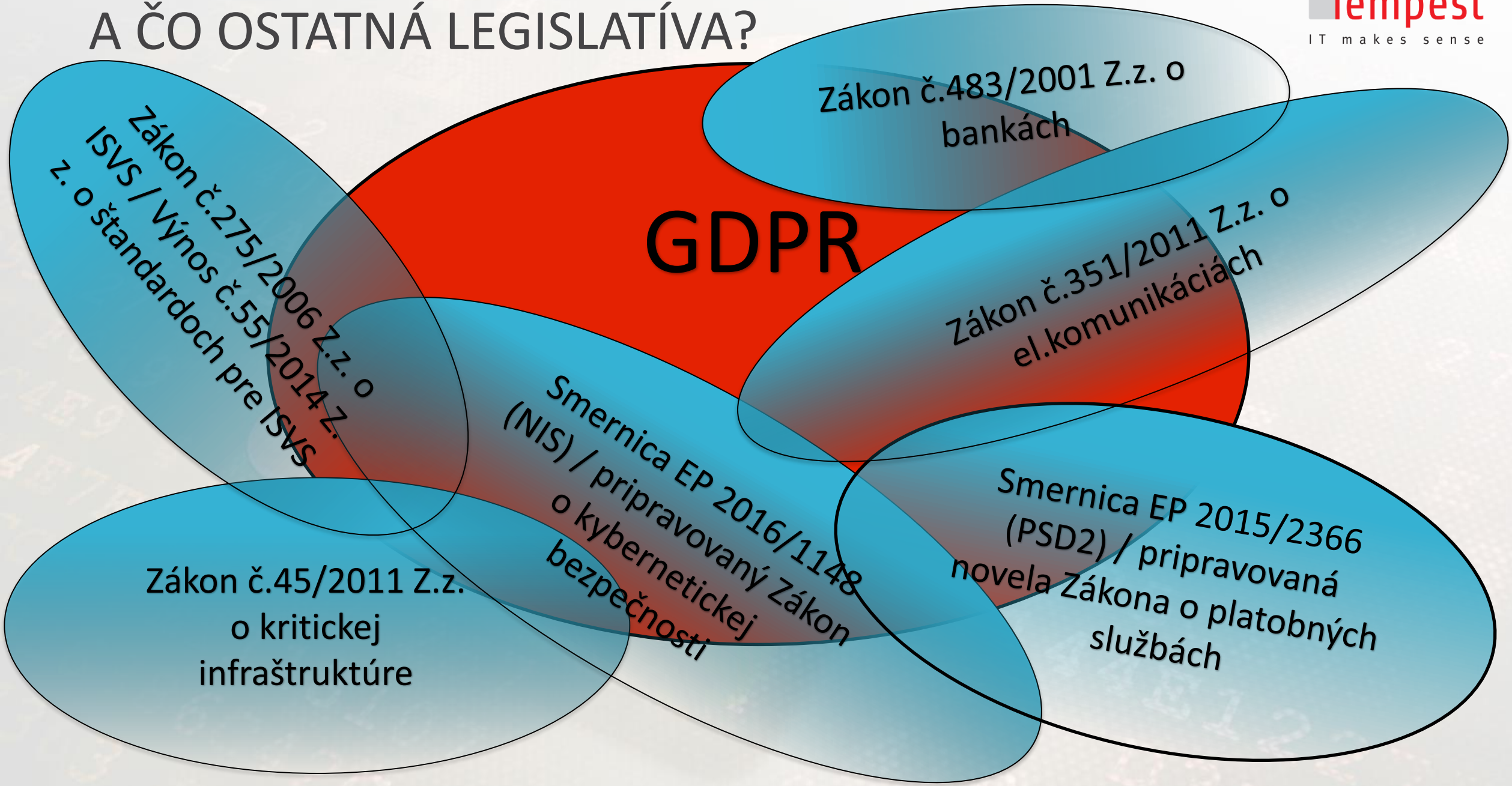
ISO

NIST National Institute of Standards and Technology U.S. Department of Commerce

enisa European Network and Information Security Agency

A ČO OSTATNÁ LEGISLATÍVA?

Tempest
IT makes sense



A ČO OSTATNÁ LEGISLATÍVA?

Tempest
IT makes sense

Výnos č. 55/2014 Z. z. o štandardoch pre ISVS

§31

„Štandardom
bezpečnosti je
a) **implemen**
overer
rizík a mo
sys
b) po
c)
d)

Zákon o bankách

§40

Banka

Zákon č. 45/2

§10, ods.1

„Rozsah bezpe

Zákon č.351/2011 Z.z. o elek

§56, ods.1

Podnik je povinný prijať

PSD2

Čl.95, ods.1

„... aby poskytovatelia platobných služieb
ustanovili rámec s vhodnými opatreniami na
zmiernenie a kontrolnými mechanizmami s **cieľom**
riadiť prevádzkové a bezpečnostné riziká súvisiace
s platobnými službami, ktoré poskytujú.“

NIS / pripravovaný zákon o kybernetickej bezpečnosti

§19, ods.3

„Bezpečnostné opatrenia sa prijímajú pre oblasť:
- **riadenia bezpečnosti a rizík**,
- personálnej bezpečnosti,
- ...“

e takto:

eb ... So zreteľom
u, **tieto opatrenia**
existujúcemu

ničenia
ta,
narušenia alebo zničenia na
uitu činnosti prvku.

A ČO OSTATNÁ LEGISLATÍVA?

Tempest
IT makes sense

Výnos č. 55/2014 Z. z. o štan
§29 - §43
Požiadavky
opatrení:
- opatreni
-
-
-
-
-

Zákon č. 45/2011 o kritickej infraštruktúre
Príloha č.2
covávaní ktorého
ch opatrení na
vestície a postupy
cieľom
sa uplatňujú v
ničenia prvku.“

Zákon č.351/2011 Z.z. o elektronických komunikáciách
§64 ods.1
„Podnik je povinný **prijať zodpovedajúce technické**
etí
abezpečiť
nu riziku.“

NIS / pripravovaný zákon o kybernetickej bezpečnosti
§19, ods.3
„Bezpečnostné **opatrenia sa prijímajú pre oblasť**:
- ...
- personálnej bezpečnosti,
- bezpečnosti systémov a zariadení,
- riadenia dostupnosti siete a informačného systému,
- monitorovania, testovania bezpečnosti a bezpečnostných auditov,
- ...“

A ČO OSTATNÁ LEGISLATÍVA?

Tempest
IT makes sense

Výnos č. 55/2014 Z.
§37
Požia
moni
ako s

Met
info
„Na
incid
jeho
zam
- **bez**
- chy
- zly
- ...“

Zákon č.351/2011 Z.z. o elektronických komunikáciách

PSD2
Čl.95, ods.1
„Poskytovatelia platobných s
účinné postupy riadenia inci
prevádzkových a bezpečnost

Čl.96, ods.1
„**V prípade závažného preva**
poskytovatelia platobných s
orgán ... Poskytovateľ platob
finančné záujmy jeho používa
informuje svojich používateľo
opatreniach, ktoré môžu prija

NIS / pripravovaný zákon o kybernetickej bezpečnosti
§18 ods. 4
„ ... prevádzkovateľ základnej služby **je povinný bezodkladne hlásiť kybernetický bezpečnostný incident** prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, riešiť tento kybernetický bezpečnostný incident a spolupracovať s úradom ...“

§21 ods. 3
Poskytovateľ digitálnej služby **je povinný prostredníctvom jednotného informačného systému kybernetickej bezpečnosti hlásiť každý kybernetický bezpečnostný incident** s významným dopadom na poskytovanie jeho služieb,

A ČO OSTATNÁ LEGISLATÍVA?

Tempest
IT makes sense

Výnos č. 55/2014 Z. z. o štandardoch pre ISVS
§37
„... **určenie osoby alebo o**
informačnú bezpečnosť p
zo
sys

Zákon č. 45/2011 o kritickej infraštruktúre
§9, ods.1
„Prevádzkovateľ je povinný ochraňovať prvok pred narušením
prevádzkovateľ je povinný:

torá je zároveň kontaktná osoba, ak
ickej infraštruktúry,

uje styk medzi prevádzkovateľom
aštruktúry, príslušným ústredným
i ochrane prvku európskej kritickej
u informácií o hrozbe jeho
narušenia alebo zničenia."

NIS / pripravovaný zákon o kybernetickej bezpečnosti
§19, ods.4
Bezpečnostné opatrenia musia zahŕňať najmenej
- ...
- riešenie kybernetických bezpečnostných incidentov,
- **určenie kontaktnej osoby pre prijímanie a evidenciu hlásení**,
- ...“

KTO PRIMÁRNE NESIE ZODPOVEDNOSŤ?

Tempest
IT makes sense

Business

- zabezpečenie zákonnosti, spravodlivosti a transparentnosti spracúvania oú
- minimalizácia oú a doby ich uchovávania
- právo na opravu oú / správnosť oú
- právo na zabudnutie
- posúdenie vplyvu spracovateľských operácií na ochranu osobných údajov
- informačná povinnosť / právo na prístup k údajom

IT opp.

- dostupnosť a obnova oú / zálohovanie oú
- prenositeľnosť oú
- incident management (monitoring)

Security

- posúdenie primeranej úrovne bezpečnosti
- zabezpečenie trvalej dôvernosti, dostupnosti, integrity a odolnosti systémov spracúvania a služieb
- implementácia primeraných organizačných a technických opatrení ako napr. šifrovanie, preudonymizácia, ...
- security incident manažment
- testovanie, posudzovanie a hodnotenie účinnosti zavedených opatrení
- posúdenie vplyvu spracovateľských operácií na ochranu osobných údajov

AKO ZOSTAVIŤ PRACOVNÝ TÍM NA IMPLEMENTÁCIU POŽIADAVIEK GDPR?

Tempest
IT makes sense

- vlastníci business procesov
- CIO/IT manažér
- manažér bezpečnosti/CSO
- špecialista na ZOOÚ/GDPR, resp. DPO (osoba zodpovedná za výkon dohľadu nad ochranou osobných údajov)
- právnik
- **MANAŽMENT**

NAJVÄČŠIE PROBLÉMY A VÝZVY

Tempest
IT makes sense

- nízke povedomie ohľadne GDPR – riešenie GDPR nie je len problém DPO ale hlavne všetkých business vlastníkov
- „zatiaľ sa nám nič nestalo“ alebo „budeme riešiť až keď vznikne problém“ – do značnej miery problém podpory manažmentu
- údaje spracúvané mimo IT systémy – excel tabuľky, dokumenty na PC, na file serveroch, ...
- spracúvanie osobných údajov navyše „len pre istotu“
- nedostatočne, resp. vôbec neupravená likvidácia osobných údajov spracúvaných v elektronickej forme
- údaje v oblakoch (cloude)
- nízke technologické povedomie sudcov

RADY A TIPY

Tempest
IT makes sense

- Implementácia GDPR je záležitosť, ktorá **musí byť vnímaná na úrovni predstavenstva i výkonného manažmentu** a realizovaná v kooperácii s business útvarmi, CIO a CSO.
- **Identifikujte súvisiacu legislatívu.**
- **Zostavte si vhodný kompetentný tím.**
- **Urobte si audit nad osobnými údajmi.** Porozumejte, ktoré dáta potrebujete a ktoré uchovávate. Porozumejte, koľko dát spracovávate a vyhodnoťte, či ich treba všetky skutočne zbierať alebo či môžu byť zmazané.

RADY A TIPY

Tempest
IT makes sense

- **Identifikujte toky osobných údajov** vo vašej organizácii a identifikujte ako sú ukladané, chránené, spracovávané a vymazávané (v papierovej aj elektronickej forme).
- Nespoliehajte sa na to, že existuje „zázračný systém“ ktorý vám vyrieši súlad s GDPR.
- Zvážte zmeny procesov, politík a informačných technológií. Tam, kde je to relevantné, prehodnoťte aj produkty a služby zahŕňajúce osobné údaje tak, aby bola **zabezpečená zhoda s nariadením GDPR.**

POTREBUJETE POMÔCŤ?

Novoprijatá regulácia má dopad aj na vašu organizáciu. Budeme s vami spolupracovať pri analýze, odporúčaniach, implementácií procesov i technológií a pri ich prevádzke.

TEMPEST má dlhoročné skúsenosti v oblasti ochrany údajov a pokrýva všetky oblasti GDPR.

Tempest
IT makes sense

DÔLEŽITÉ ODKAZY

www.tempest.sk/gdpr

www.tempest.sk/gdpr-odporucania

www.eugdpr.org

Tempest

IT makes sense