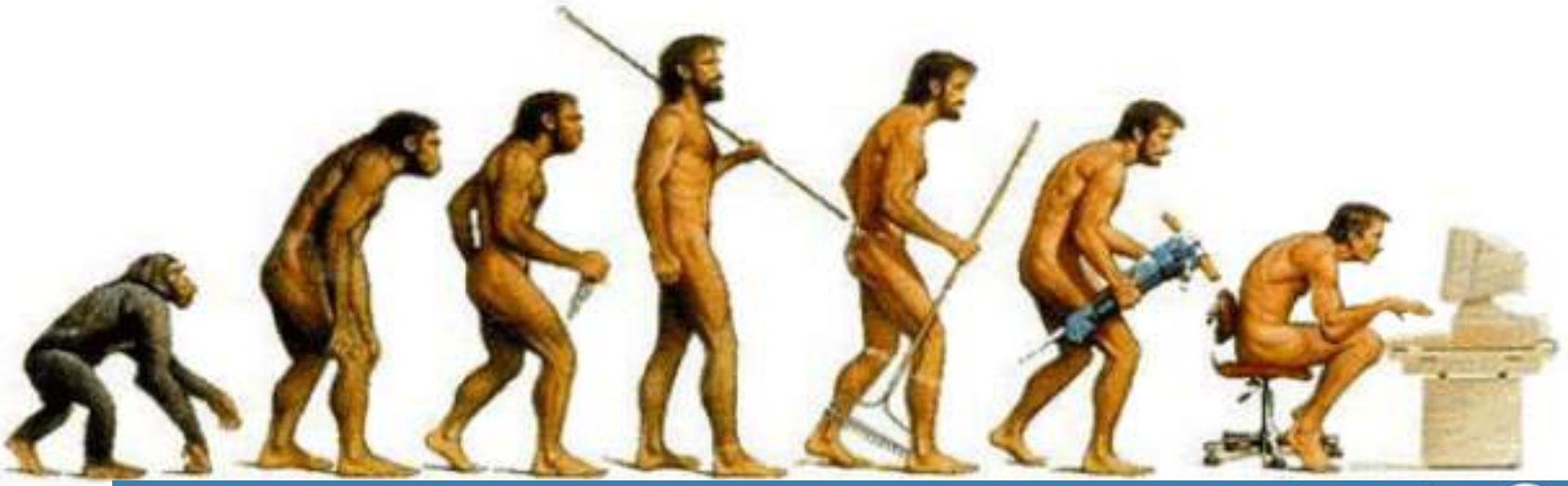
ÚSKALÍ IMPLEMENTACE GDPR

Jan Kolouch

GDPR



https://dataf loq.com/rea d/7-trends- of-internet- of-things-in- 2017/2530

https://pbs.twimg.com/media/C7T8TisXUAAEHiU.jpg

CESNET

CÍL GDPR

- komplexní úprava ochrany osobních údajů (ne jen v EU)
- jednotný právní rámec, výklad
- rovnováha mezi oprávněnými zájmy správců, zpracovatelů a subjektů údajů
- jednotná vymahatelnost práva v EU
- jednotný sankční mechanismus
- spolupráce dozorových orgánů

One Ring to rule them all,
One Ring to bring them all…

DOSAH GDPR?

GDPR se uplatní v případech, kdy je:

- provozovna správce nebo zpracovatele v EU, bez ohledu na to, zda zpracování probíhá v EU
- správci nebo zpracovatelé neusazení v EU
  - zboží nebo služby jsou nabízeny subjektům údajů v EU (bez ohledu na úplatu)
  - monitorováno chování subjektů údajů v rámci EU

Google

KDO A CO JE VLASTNĚ CHRÁNENO?

SUBJEKT ÚDAJŮ

Čl. 4 odst. 1

Subjektem údajů je *identifikovaná nebo identifikovatelná* ***fyzická osoba.***

Identifikovatelnou *fyzickou osobou* ***je fyzická osoba, kterou lze přímo či nepřímo identifikovat***

OSOBNÍ ÚDAJ

Čl. 4 odst. 1 GDPR

*veškeré **informace o identifikované nebo identifikovatelné fyzické osobě.***

Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat

*zejména **odkaz na určitý identifikátor**, například **jméno**, **identifikační číslo**, **lokační údaje**, **síťový identifikátor nebo na jeden či více zvláštních prvků** fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské **identity této fyzické osoby.***

Čl. § 4 ZOOU

a) osobním údajem jakákoliv informace týkající se **určeného nebo určitelného subjektu údajů.**

Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat

zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,

VLASTNÍ POJEM OSOBNÍ ÚDAJ NEBYL OPROTI ZOOU DE FACTO ZMĚNĚN.

OSOBNÍ ÚDAJ

- veškeré **informace** (**obrazové, písemné, slovní, digitální, genetické, zdravotnické aj.**),
- **mající vztah** (obsahem – např. **jméno, adresa, pracovní zařazení, email aj.**),
- **k subjektu údajů.**

Subjekt může být identifikován:

- přímo
- nepřímo (např. **výběr vyčleněním** aj.)

OSOBNÍ ÚDAJ

Osobní:

- **jméno a příjmení**
- **identifikační číslo**
- **RČ**
- **lokační údaje** (geo-)
- **věk a datum narození**
- **pohlaví**
- **osobní stav**
- **občanství**
- **IP adresa**
- **fotografie**
- **prvky** fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské **identity**

Organizační:

- pracovní/osobní **adresa**
- pracovní/osobní **telefonní číslo**
- pracovní/osobní **email**
- **ověřovací identifikační údaje**
- **identifikační čísla vydaná státem**

V30

https://www.gdpr.cz/gdpr/heslo/osobni-udaje/

OSOBNÍ ÚDAJ

Citlivý osobní údaj:

- rasovém či etnickém **původu**
- **vyznání**
- **politických názorech**
- **členství** v odborech či jiných organizacích
- **sexuální orientaci**
- spáchání deliktů (trestný čin/přestupek aj.) a potrestání za ně

Další údaje:

- **genetické údaje** (DNA & RNA)
- **biometrické údaje**
- **údaje o zdravotním stavu**
- **OÚ dětí**

V34, 35, 38, 53

OSOBNÍM ÚDAJEM JE I ŠIFROVANÝ OÚ.

OSOBNÍ ÚDAJ O ZDRAVOTNÍM STAVU

Veškeré údaje:

- **související se zdravotním stavem subjektu údajů**, které vypovídají o:
  - **minulém, současném či budoucím**
  - **tělesném nebo duševním zdraví subjektu údajů**

Informace získané:

- **v průběhu registrace** pro účely zdravotní péče
- **v průběhu poskytování zdravotní péče**

Jde tedy o:

číslo, symbol nebo **specifický údaj přiřazený fyzické osobě** za účelem její jedinečné identifikace pro zdravotnické účely, **informace získané během provádění testů nebo vyšetřování části těla nebo tělesných látek**, včetně z genetických údajů a biologických vzorků, a **jakékoliv informace například o nemoci, postižení, riziku onemocnění, anamnéze, klinické léčbě nebo fyziologickém či biomedicínském stavu subjektu údajů nezávisle na jejich původu**, tedy bez ohledu na to, zda pocházejí například od lékaře nebo jiného zdravotníka, z nemocnice, ze zdravotnického prostředku či diagnostických testů in vitro.

CO MŮŽE SUBJEKT OÚ ŽÁDAT?

- **přístup k OÚ**
- **být informován o zpracování (kdo, co, kde, kdy, jak dlouho, proč, kam?…)**
  - Účely zpracování
  - Kategorie údajů
  - Příjemci
  - Doba uchování
  - Existence práva na výmaz, omezení, námitku či stížnost
  - Informace o zdroji
  - Profilování/automatizované rozhodování

  (Řešeno již stávající právní úpravou)
- **právo na opravu, výmaz, omezení, přenesení údajů**

  (Nově řešeno GDPR).

PROBLÉMY

INFRASTRUKTURA PRO VÝZKUM DATOVÝCH ÚLOŽIŠŤ

- **Identifikace a kategorizace OÚ**
  - **„běžné OÚ“**
    - IP adresa, ID, email aj.
  - **zvláštní kategorie OÚ**
    - Předmět výzkumu, přiřaditelný subjektu údajů aj.
- **Ochrana osobních údajů**
- **Správa přístupu**
- **Stanovení doby a účelu**
- **Right to be forgotten**

IP ADRESA = OSOBNÍ ÚDAJ?

Patrick Breyer proti **Bundesrepublik Deutschland**

http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270

dynamická IP adresa je dle rozsudku soudního dvora EU z 19.10.2016 za určitých okolností osobním údajem

JSEM 100 % SCHOPEN ODLIŠIT:

- MAN TO MACHINE
- MACHINE TO MACHINE

KOMUNIKACI?

DHCP

IP připojovacího prvku (např. AP aj.)

MAC adresa PC uživatele

IP přidělené PC

Jméno PC uživatele nastavené v OS

Sep 4 15:40:09 dhcp dhcpd: DHCPDISCOVER from d0:[redacted]:d4 (corwin) via 195.113.219.131

Sep 4 15:40:10 dhcp dhcpd: DHCPOFFER on 195.113.[redacted].206 to d0:[redacted]:d4 (corwin) via 195.113.[redacted].131

Sep 4 15:40:10 dhcp dhcpd: DHCPREQUEST for 195.113.[redacted].206 (78.128.211.148) from d0:[redacted]:d4 (corwin) via 195.113.[redacted].131

Sep 4 15:40:10 dhcp dhcpd: DHCPACK on 195.113.[redacted].206 to d0:[redacted]:d4 via 195.113.[redacted].131

IP DHCP

IP PC uživatele

Ověření uživatele

Jedinečný identifikátor

email uživatele

Sep 7 10:48:03 office2 postfix/smtps/smtpd[22748]: connect from unknown[2001:718:2:2226:d27e:[redacted]d4]
Sep 7 10:48:03 office2 postfix/smtps/smtpd[22748]: Anonymous TLS connection established from unknown[2001:718:2:2226:d27e:[redacted]d4]: TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits)
Sep 7 10:48:03 office2 postfix/smtps/smtpd[22748]: D615B400063 : client=unknown[2001:718:2:2226:d27[redacted]d4], sasl_method=PLAIN, sasl_username=andrea
Sep 7 10:48:03 office2 postfix/cleanup[21618]: D615B400063 : message-id=<alpine.LFD.2.20.1709071044480.3384@corwin.cesnet.cz >
Sep 7 10:48:03 office2 postfix/qmgr[1919]: D615B400063: from=<andrea@cesnet.cz >, size=1591, nrcpt=1 (queue active) (zpracování zprávy)
Sep 7 10:48:03 office2 postfix/smtps/smtpd[22748]: disconnect from unknown[2001:718:2:2226:d27e:[redacted]d4] ehlo=1 auth=1 mail=1 rcpt=1 data=1 quit=1 commands=6
Sep 7 10:48:03 office2 postfix/smtp[22213]: D615B400063 : to=<masters@cesnet.cz>, relay=postino.cesnet.cz[2001:718:1:[redacted]::[redacted]:242]:25, delay=0.07, delays=0.06/0/0.01/0, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as E4DFD58007F)
Sep 7 10:48:03 office2 postfix/qmgr[1919]: D615B400063: removed

Identifikátor emailu

IP Serveru

HTTP

IP PC uživatele

email uživatele

Identifikace browseru. **Neotagovaná**

2001:718:1:6::[redacted]:231 - - [07/Sep/2017:10:15:05 +0200] "GET /Shibboleth.sso/Login?SAMLDS=1&target=https%3A%2F%2Fmx.cesnet.cz%2F&entityID=https://whoami.cesnet.cz/idp/shibboleth&filter=eyJhbGxvd0ZlZWRzIjogWyJlZHVJRC5jeiJdLCAiYWxsb3dIb3N0ZWwiOiB0cnVlLCAiYWxsb3dIb3N0ZWxSZWciOiB0cnVlfQ%3D%3D HTTP/1.1" 302 6772 "https://ds.eduid.cz/wayf.php?filter=eyJhbGxvd0ZlZWRzIjogWyJlZHVJRC5jeiJdLCAiYWxsb3dIb3N0ZWwiOiB0cnVlLCAiYWxsb3dIb3N0ZWxSZWciOiB0cnVlfQ==&entityID=https%3A%2F%2Fmx.cesnet.cz%2Fsp%2Fshibboleth&return=https%3A%2F%2Fmx.cesnet.cz%2FShibboleth.sso%2FLogin%3FSAMLDS%3D1%26target%3Dhttps%253A%252F%252Fmx.cesnet.cz%252F" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36 "

2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET / HTTP/1.1" 200 21914 "https://whoami.cesnet.cz/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZJdT4MwFIb%2FCun9KBAZ0gwS3C5cMh0Z6IU3pitn0gRa7ClO%2FfWyMXUmZtd9P877pDPkbdOxrLe12sBrD2id97ZRyI4PCemNYpqjRKZ4C8isYEV[redacted]owb1LAw2aVkNraDhml7bsrABVYV3zSopbbrW7A1i6ipofMgObroiTOYjhCKn6I%2BzXva81beRYgq44OB%2BxkAyf3I[redacted]RGEUBDyO%2FXgqeBCK6kpMvUGG2MNSoeXKJiTw%2FGjixRMvKr1r5ofMC5%2BIk5923khVSfVyGcp2FCG7Lct8Mi[redacted]Ilk%2FZcndhR%2FkM7oWcXY17H7IXO5yHUjxYeTNY3ezw1wCwnxCU1Hy9%2BfkH4B&RelayState=https%3A%2F%[redacted]2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=YSkFyVi2HbzZUpyzC2x207wLfLdzNESo9OqjuxGX3Em[redacted]5gNnm51jjx0UValE78YRPaz70rND8Rog%2F%2FU%2BT9Z9NvZay3pKOhrvSVs4VLl%2FM7eMeg5VbwqlNowHSWbw11fFG%2BoSnuk%2F5Nq1Dg9KQezwyw8na4O2wmtzdsbtS6%2B0yuTtil3bFfjuLzUHWvWQ1%2BAtQo%2BVc9%2BKsVnfYWWU84yVlMsei6wAWZuy1noe9ssRIU9ajf4%2FKZ[redacted]ZAIwbeemz2uKC9UlSGY6pYjae938s%2BY9MbzaaEm%2Brycwlz9viM4eBD7urRz%2BV2QjSt4ZvQ%3D%3D" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET /css/style.css HTTP/1.1" 200 956 "https://mx.cesnet.cz/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET /css/jquery.dataTables.css HTTP/1.1" 200 2923 "https://mx.cesnet.cz/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET /js/jquery-latest.min.js HTTP/1.1" 200 33812 "https://mx.cesnet.cz/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET /js/highcharts.js HTTP/1.1" 200 62110 "https://mx.cesnet.cz/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET /js/jquery.dataTables.js HTTP/1.1" 200 113792 "https://mx.cesnet.cz/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET /img/sort_both.png HTTP/1.1" 200 549 "https://mx.cesnet.cz/css/jquery.dataTables.css" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

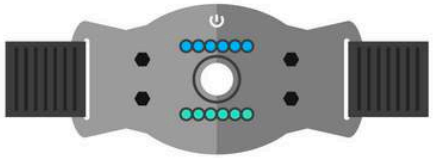
2001:718:1:6::[redacted]:231 - user@cesnet.cz [07/Sep/2017:10:15:06 +0200] "GET /img/sort_asc.png HTTP/1.1" 200 508 "https://mx.cesnet.cz/css/jquery.dataTables.css" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"

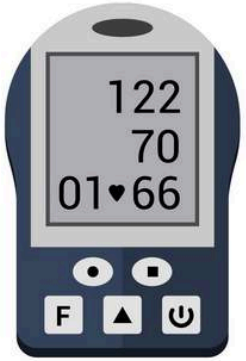

GPS
tracker


118


John


120




122
70
01♥66
F

OCHRANA OÚ

Správce a zpracovatel jsou povinni provést vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku s přihlédnutím:

- **ke stavu techniky,**
- **nákladům na provedení,**
- **povaze, rozsahu, kontextu a účelům zpracování i**
- **k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob"**

Záměrná ochrana = By design (individualizace ochrany)

Implementace prostředků, jak v době určení, tak při zpracování samotném, aby byly splněny požadavky GDPR (např. pseudonymizace, minimalizace OÚ, transparentnost aj.)

Standardní ochrana = By default (zpracování na základě účelu)

Zajištění, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. *Opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob. (množství, rozsah, doba, dostupnost)*

Čl. 25

SPRÁVA PŘÍSTUPU

- **A**uthentication, **A**uthorization, **A**ccounting protocol
  - **Active directory?**
  - **Nastavení pravidel pro přístup k jednotlivým OÚ**
- **Replikace dat**
- **Cloudová řešení**
- **Šifrování**

ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Pokud jsou osobní údaje získávány od subjektu údajů, **měl by subjekt údajů být rovněž informován, zda je povinen tyto ú**

n

Z

u

-

-

-

- **podávané za použití jasných a jednoduchých jazykových prostředků** a **ve vhodných případech navíc i vizualizace**.

58, 60

https://hollandfintech.com/privacy-valley-reviews-compliance-issues-in-series-reconciling-psd2-gdpr/

PRÁVO SUBJEKTŮ ÚDAJŮ NA PŘÍSTUP K ÚDAJŮM O SVÉM ZDRAVOTNÍM STAVU

Jedná se například o:

- **údaje ve své lékařské dokumentaci**
- **informace o diagnóze**
- **výsledky vyšetření**
- **posudky ošetřujících lékařů**
- **údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích.**

Každý subjekt údajů by proto měl mít **právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, případně období, po které budou uchovávány, kdo jsou příjemci** osobních údajů, **v čem spočívá logika automatizovaného zpracování osobních údajů a jaké mohou být důsledky takového zpracování přinejmenším v případech, kdy je zpracování založeno na profilování.**

PROCES ŽÁDOSTI

Je třeba stanovit postupy, které by **usnadnily výkon práv subjektů** údajů podle GDPR, **včetně mechanismů pro podávání žádostí a případně bezplatného obdržení přístupu k osobním údajům a opravy nebo výmazu osobních údajů a pro uplatnění práva vznést námitku.**

Správce by měl:

- **umožnit podávání žádostí elektronicky**, zejména v případě zpracování osobních údajů elektronickými prostředky.
- **reagovat na žádosti bez zbytečného odkladu**
- **nejpozději do jednoho měsíce**
- **uvést důvody v případě, že nemá v úmyslu těmto žádostem vyhovět.**

V59

VLASTNÍ PŘÍSTUP?

Je-li to možné, měl by správce:

- poskytnout dálkový **přístup k bezpečnému systému, který by subjektu údajů umožnil přímý přístup k jeho osobním údajům**

Tím by neměla být nepříznivě dotčena práva ani svobody ostatních, například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení.

Zohlednění těchto skutečností by ovšem nemělo vést k tomu, že by subjektu údajů bylo odepřeno poskytnutí všech informací.

V případě, že správce zpracovává velké množství informací týkajících se subjektu údajů:

- **možnost požádat subjekt údajů** (před vlastním poskytnutím informací)**, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká.**

V63

RIGHT TO BE FORGOTTEN

Aby bylo v internetovém prostředí posíleno právo být zapomenut, mělo by být rozšířeno právo na výmaz tím, že by správce, který zveřejnil osobní údaje **měl povinnost informovat správce, kteří osobní údaje zpracovávají, aby vymazali veškeré odkazy na dané osobní údaje či veškeré jejich kopie nebo replikace.**

V66

Subjekt požaduje změny, opravy, výmaz aj. po SPRÁVCI.

Toto právo není absolutní

PŘENOSITELNOST OÚ

- **Pokud je zpracování:**
  - **založeno na souhlasu subjektu OÚ**
  - **provádí se automatizovaně,**

má subjekt právo získat osobní údaje, které se ho týkají, a jež poskytl správci, **ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu** a předat je jinému správci, i bez souhlasu původního správce.

Výjimky:

- **zpracování nezbytné ve veřejném zájmu**, nebo
- **při výkonu veřejné moci**

Čl. 20, V68

PORUŠENÍ ZABEZPEČENÍ OÚ

V oznámení musí být popsána:

- **povaha daného případu porušení zabezpečení osobních údajů**
- **doporučení pro dotčenou fyzickou osobu, jak případné nežádoucí účinky zmírnit**

oznámení by měla být subjektu údajů učiněna, jakmile je to proveditelné, v úzké spolupráci s dozorovým úřadem a v souladu s pokyny tohoto úřadu nebo jiných příslušných orgánů

V86

Nastavení procesů zejména ve vztahu ke službám poskytovaným v souvislosti s využíváním ICT.

VHODNÝ POSTUP

- **ORGANIZACE JAKO CELEK**
  - provedení auditu, kde všude se pracuje s OÚ ve vztahu k GDPR
  - **tvorba pravidel a procesů UVNITŘ ORGANIZACE**
  - **tvorba NOVÝCH pravidel a procesů VE VZTAHU K SUBJEKTU OÚ**
    - Stanovení podmínek dle GDPR (jasné srozumitelné atd.)
    - Stanovení účelu pro každé zpracování OÚ
    - Možnost nesouhlasu subjektu údajů
  - **DPO?**

Spolupráce při tvorbě pravidel a jejich implementaci

GDPR...

OCHRANA OSOBNÍCH ÚDAJŮ

V JAKÉKOLIV FORMĚ

„ZA KAŽDOU CENU…“

25. 5. 2018

Děkuji za pozornost

JUDr. Jan Kolouch, Ph.D.
sdružení CESNET, z.s.p.o.
jan.kolouch@cesnet.cz

SEZNAM ZKRATEK

OÚ = osobní údaje

SÚ = subjekt údajů

ZOOU = zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

V = vysvětlivka GDPR

Čl. = článek GDPR