

Praktické skúsenosti z implementácie GDPR v stredne veľkých organizáciách

Ing. Robert Maier
analytik

Implementácia GDPR

...aký je dopad nariadenia na technické informačné systémy...

Obsah prezentácie

Čo by som Vám chcel dnes povedať



OBLASŤ ZÁUJMU

- Úvod do elektroenergetiky
- Pozícia spoločnosti sféra, a.s.



POSTUP IMPLEMENTÁCIE

- Dotknuté informačné systémy
- Ako chápeme osobné údaje
- Ako pripraviť informačný systém na GDPR
- Súčasný stav



ČO MÁME PRED SEBOU

+Záležitosti, ktoré nás dostali do rozpakov...

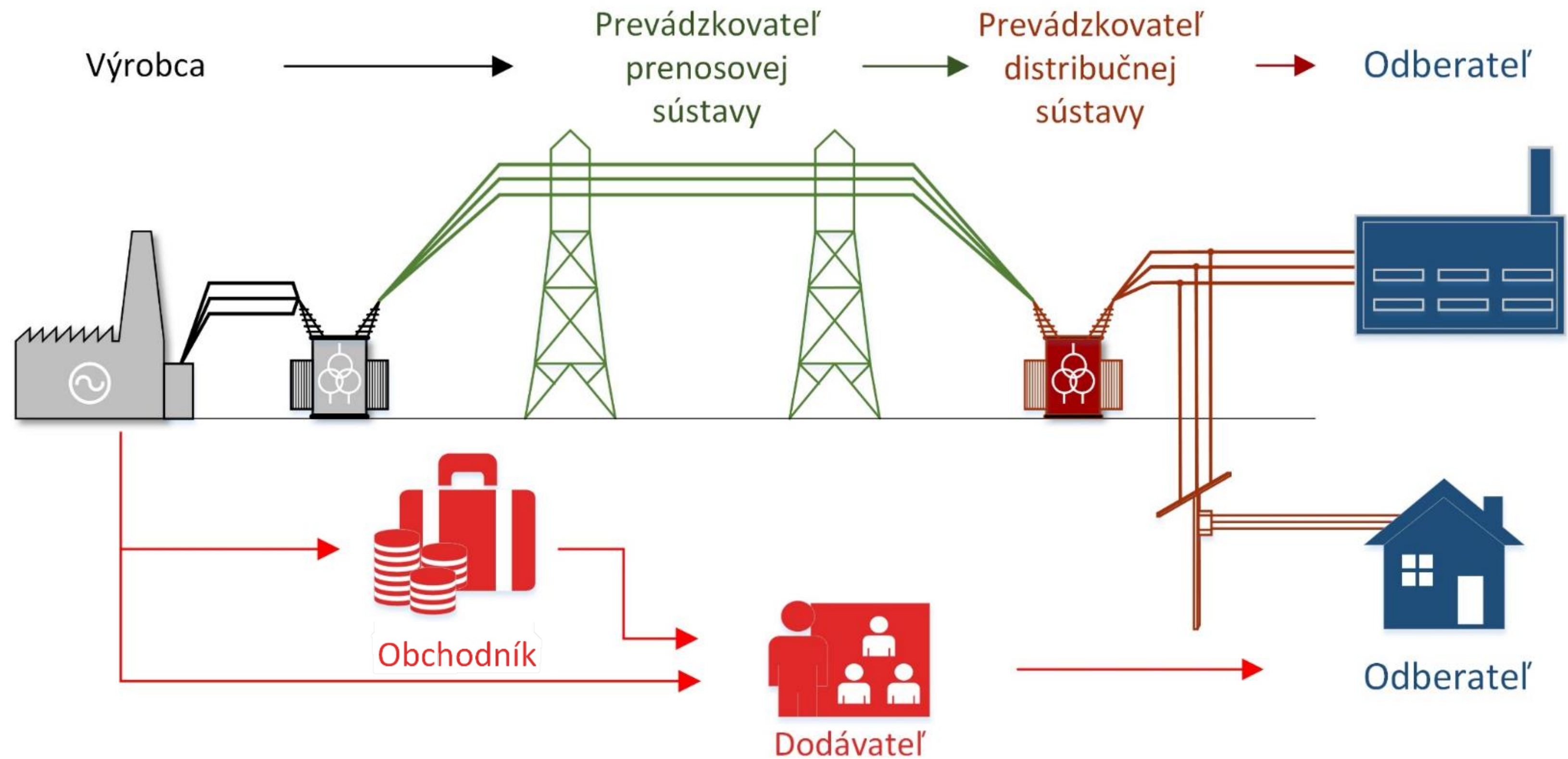


ZRHNUTIE

Myšlienky nad ktorými treba premýšľať...

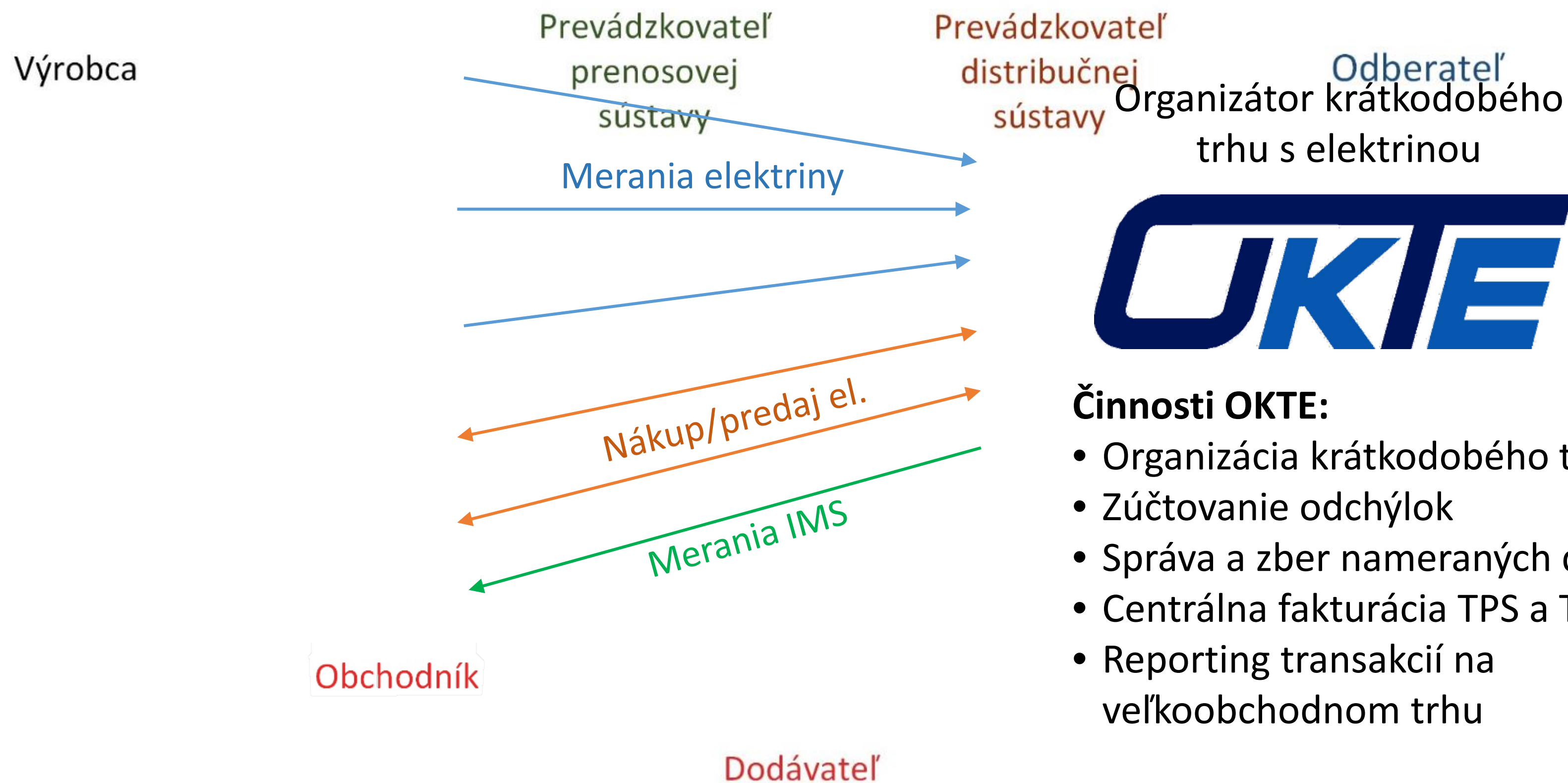
Oblasť záujmu

Úvod do elektronenergetiky



Oblasť záujmu

Úvod do elektronenergetiky

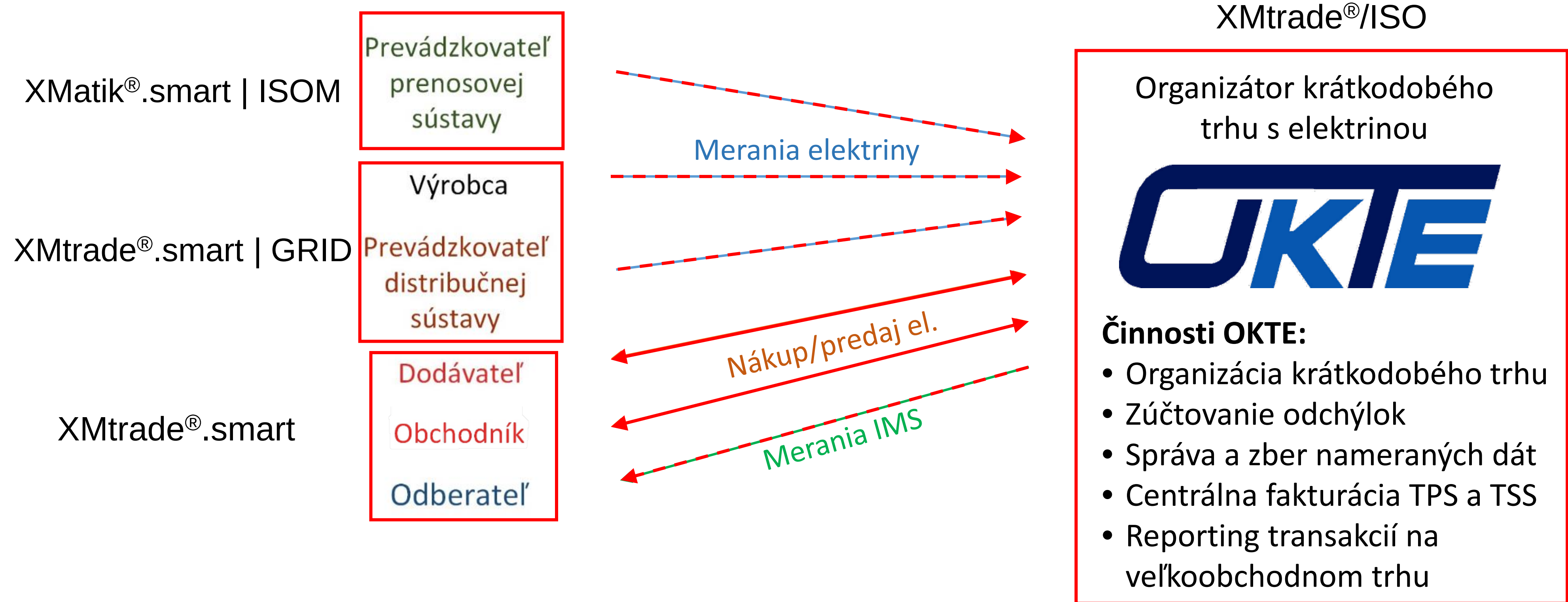


Činnosti OKTE:

- Organizácia krátkodobého trhu
- Zúčtovanie odchýlok
- Správa a zber nameraných dát
- Centrálna fakturácia TPS a TSS
- Reporting transakcií na veľkoobchodnom trhu

Oblasť záujmu

Spoločnosť sféra, a.s. v elektroenergetike



Oblasť záujmu

Spoločnosť sféra, a.s. v elektroenergetike

sféra, a.s. ako dodávateľ IT riešení je z pohľadu nariadenia GDPR voči svojim zákazníkom v roli **sprostredkovateľ**.

Postup implementácie

Dotknuté informačné systémy

Informačný systém	Pokrytie činností	Obsahuje OÚ
XMtrade® / ISOT	Organizácia krátkodobého trhu	x
XMtrade® / ISZO	Zúčtovanie odchýlok	x
XMtrade® / ISOM	Správa a zber nameraných údajov	✓
XMtrade® / IMS	Poskytovanie meraní odberateľom s IMS	✓
XMtrade® / RRM	Reporting veľkoobchodných transakcií	x
XMtrade®.smart	Činnosti dodávateľov a obchodníkov	✓
XMtrade®.smart GRID	Činnosti miestnych distribučných sústav	✓
XMatik®.smart ISOM	Obchodné merania prevádzkovateľa PS	x

Postup implementácie

Ako pripraviť informačný systém, ale aj firmu, na GDPR

- ✓ Poradiť si s GDPR naprieč celou firmou
- ✓ Odlíšiť a chrániť osobné údaje, napr. pseudonymizáciou
- ✓ Kontrolovať, kto sa k údajom dostane a ako s nimi manipuluje
- ✓ Generovať potrebné výpisy, archivovať požiadavky osôb, umožniť vymazanie
- ✓ Sledovať, archivovať všetku manipuláciu s dátami vrátane zobrazenia
- ✓ Zohľadniť udelené súhlasy aj nakladanie s informáciami podľa zmlúv či zákona
- ✓ Chrániť osobné údaje naprieč rôznymi procesmi

Postup implementácie

Ako chápeme osobné údaje

„Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, ktorú je možné identifikovať priamo alebo nepriamo“

Nariadenie EÚ 2016/679

„Osobné údaje sú informácie, na základe ktorých sa viem dopátrať konkrétnej osoby a teoreticky jej znepříjemniť život“

Robert Maier, sféra, a.s.

Postup implementácie

Ako chápeme osobné údaje

Údaje v technických informačných systémoch sú najčastejšie kontaktné údaje.

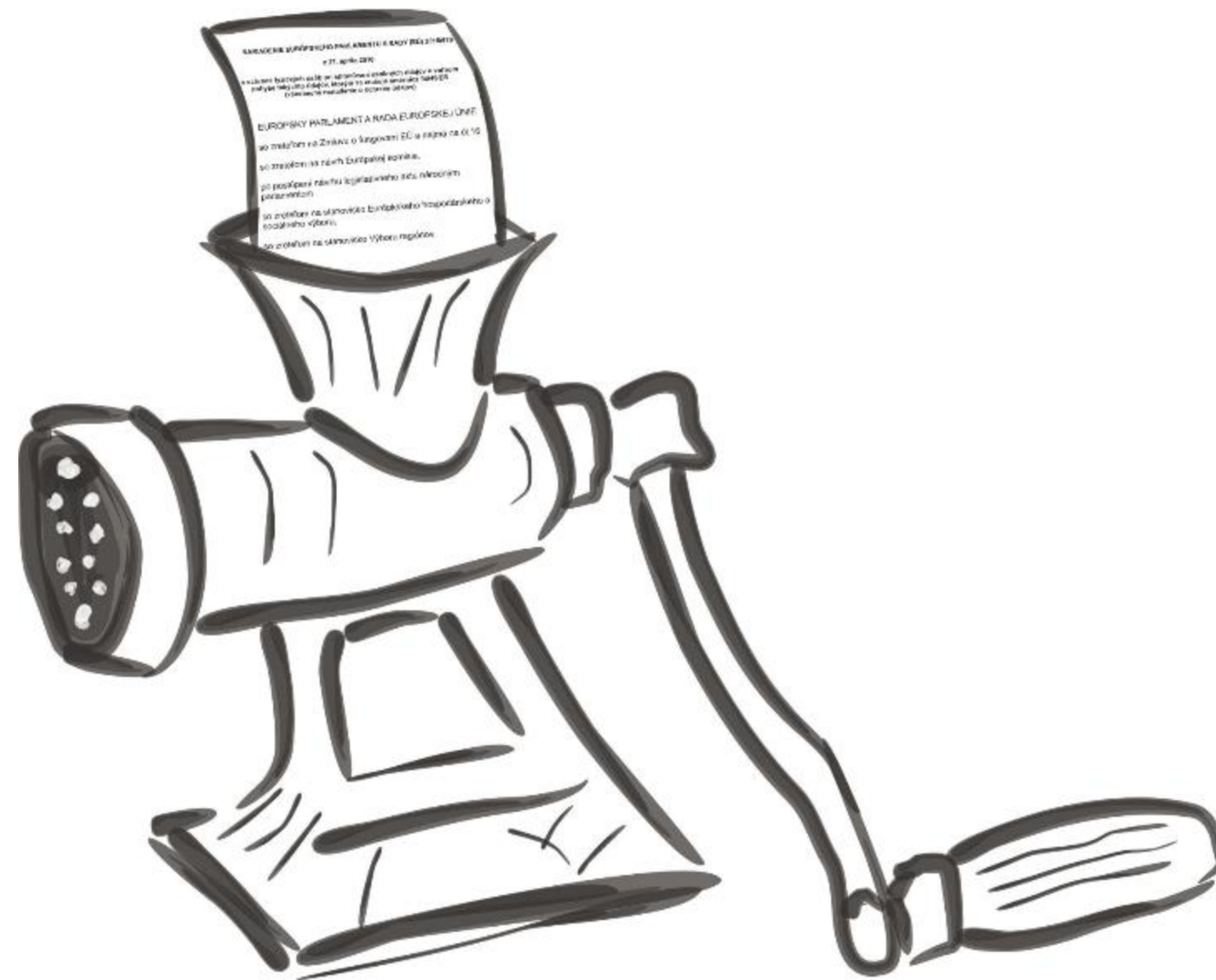
Meno + priezvisko + ...

...telefón, email, fax, adresa, ...

- Údaje fyzických osôb pôsobiacich v energetike
 - Odberatelia
 - Výrobcovia elektriny
- Používatelia systému
 - Fyzické osoby vystupujúce za seba (malí výrobcovia)
 - Zamestnanci právnických subjektov

Postup implementácie

Súčasný stav pokrytia požiadaviek GDPR



- ✓ Identifikácia dotknutých systémov
 - ✓ Identifikácia OÚ v dotknutých systémoch
- Analýza OÚ na základe ich spracúvania
- Požiadavky GDPR pre prácu s OÚ
- Zabezpečenie povinností sprostredkovateľa

Postup implementácie

Analýza osobných údajov na základe ich spracúvania

GDPR:

- Nepotrebné osobné údaje by spracúvané byť nemali
- Potrebné osobné údaje môžu byť spracúvané:
 - na základe legislatívnej povinnosti,
 - bez právneho základu.

Náš prístup:

- Prečistenie osobných údajov na tie, ktoré sú nevyhnutné
- Vytvorenie evidenčných listov
- Evidencia účelov spracúvania OÚ na základe používateľských profilov
- Vyžiadanie udelenia súhlasu dotknutou osobou so spracovaním OÚ spracovávaných bez právneho základu

Postup implementácie

Vytvorenie evidenčných listov

Evidenčný list identifikuje:

- Informačný systém
- Rozsah osobných údajov
- Účel spracúvania
- Právny základ spracúvania
- Okruh dotknutých osôb
- ...

EVIDENCIA INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

podľa § 43 ods. 1 zákona č. 122/2013 Z. z.
o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

I. NÁZOV INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV	
IS XMtrade®/ISOM	
II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	OKTE, a.s.
Identifikačné číslo organizácie (IČO)	45687862
Obec a PSČ	Bratislava 821 09
Ulica a číslo	Mlynské nivy 48
Štát	Slovenská republika
Právna forma	Akciová spoločnosť
Statutárny orgán prevádzkovateľa	
Zástupca prevádzkovateľa	
Počet oprávnených osôb	
III. ÚDAJE O INFORMAČNOM SYSTÉME OSOBNÝCH ÚDAJOV	
Účel spracúvania osobných údajov	Poskytovanie služieb, súvisiacich s výrobou elektriny z obnoviteľných zdrojov energie, napr. zber a vyhodnocovanie meraní výrobcov elektriny z obnoviteľných zdrojov energie s celkovým inštalovaným výkonom do 10 kW vrátane, ktorí si uplatňujú podporu výroby elektriny doplatkom a ktorí sú zároveň odberateľom v domácnosti
Právny základ spracúvania osobných údajov	Vyhláška č. 24/2013 Z. z. Vyhláška Úradu pre reguláciu sieťových odvetví, ktorou sa ustanovujú pravidlá pre fungovanie vnútorného trhu s elektrinou a pravidlá pre fungovanie vnútorného trhu s plynom § 37, § 12 odsek 5, 8, 10, 14 § 7 bod 5 Zákona č. 309/2009 Z. z. Zákon o podpore obnoviteľných zdrojov energie a vysoko účinnej kombinovanej výroby a o zmene a doplnení niektorých zákonov
Okruh dotknutých osôb	Výrobcovia elektriny – fyzické osoby, ktoré majú oprávnenie na výrobu elektriny podľa zákona 251/2012 Z. z. Zákon o energetike a o zmene a doplnení niektorých zákonov (osoby, ktoré vykonávajú činnosti podľa odseku 2 a 4 § 4 Zákona 251/2012 Z. z.) Užívateľ sústavy – osoba, ktorá odoberá elektrinu alebo dodáva elektrinu prostredníctvom prenosovej sústavy alebo distribučnej sústavy, alebo má s jej prevádzkovateľom zmluvný vzťah
Zoznam osobných údajov (alebo rozsah)	• Meno, priezvisko, titul • Telefón (mobil) • E-mail • Miesto podnikania
Označenie bezpečnostných opatrení	

Postup implementácie

Vyžiadanie súhlasu so spracovaním osobných údajov

 **XMtrade® / IMS**

Testovacie prostredie

Súhlas so spracovaním osobných údajov

Udeľujem spoločnosti OKTE, a.s., so sídlom Mlynské nivy 48, 821 09 Bratislava, Slovenská republika, IČO: 45 687 862, zapísanej v Obchodnom registri Okresného súdu Bratislava I, oddiel: Sa, vložka č. 5087/B („OKTE“) súhlas so spracúvaním svojich osobných údajov podľa § 11 zákona č. 122/2013 Z. z., o ochrane osobných údajov a o zmene a doplnení niektorých zákonov so spracúvaním mojich osobných údajov preukázateľne poskytnutých OKTE, najmä mena, priezviska, adresy, e-mailovej adresy a telefónneho čísla, za účelom vytvorenia prístupového účtu k webovému sídlu XMtrade®/IMS a sprístupňovania údajov o odbernom mieste koncovému odberateľovi elektriny a o priebehových a nepriebehových meraniach na tomto odbernom mieste. Súhlas udeľujem na dobu nevyhnutne potrebnú na dosiahnutie účelu spracúvania.

Vyhlasujem, že poskytnutie uvedených údajov je dobrovoľné a beriem na vedomie, že svoj súhlas so spracovaním údajov môžem bezplatne a kedykoľvek odvolať elektronicky na adrese isom@okte.sk alebo písomne na adrese OKTE, a.s., Mlynské nivy 48, 821 09 Bratislava.

Zároveň súhlasím, aby povinnosť OKTE informovať ma o spracovaní osobných údajov prostredníctvom tretích strán, bola splnená aj ich zverejnením na [webovom sídle OKTE](#). Potvrdzujem, že OKTE ma informoval o podrobnostiach o spracúvaní osobných údajov vrátane poučenia o právach dotknutej osoby na svojom [webovom sídle](#).

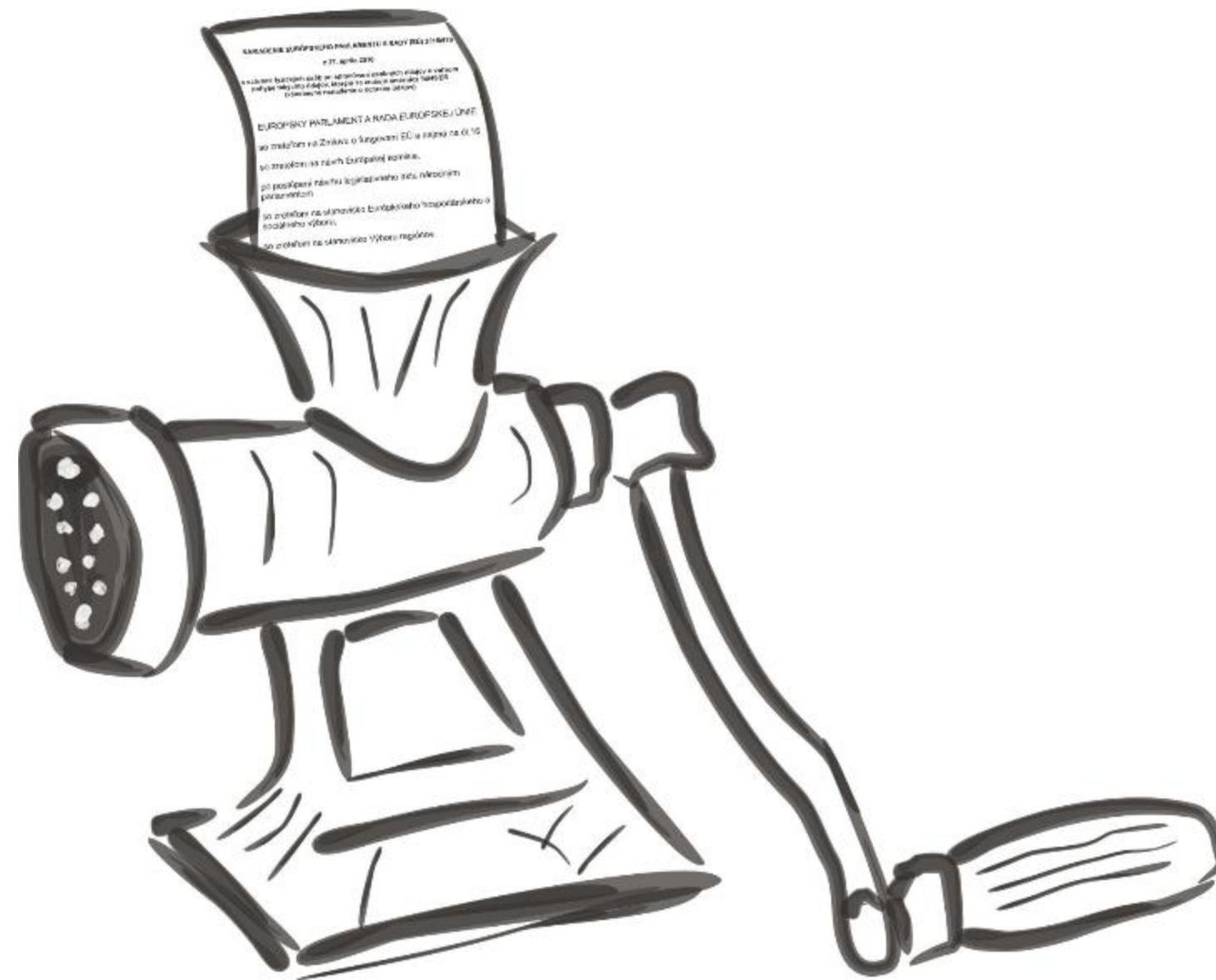
Copyright © 2017 OKTE, a.s.

5. 12. 2017 08:36:59

Design and Technology by [sféra, a.s.](#)

Postup implementácie

Súčasný stav pokrytia požiadaviek GDPR



- ✓ Identifikácia dotknutých systémov
 - ✓ Identifikácia OÚ v dotknutých systémoch
 - ✓ Analýza OÚ na základe ich spracúvania
- Požiadavky GDPR pre prácu s OÚ
- Zabezpečenie povinností sprostredkovateľa

Postup implementácie

Požiadavky GDPR pre prácu s osobnými údajmi

GDPR:

- Sprístupnenie všetkých spracúvaných OÚ dotknutej osobe
- Evidencia poskytnutých súhlasov so spracovaním OÚ
- Evidencia a realizácia požiadaviek na zabudnutie

Náš prístup:

- Vytvorenie modulu „Osobné údaje“ pre dotknuté systémy

Postup implementácie

Vytvorenie modulu *Osobné údaje*

 **Xtrade® / ISOM**

Testovacie prostredie



Úvodné okno | Obnoviť

5. 12. 2017 08:33:59 | Pomoc | Robert Maier

Navigácia

Správa exportu

Správa importu

ISOM

Zoznamy EIC

Účastníci trhu

Požiadavky IMS

Osobné údaje

Bilančné skupiny

Sústavy

Výrobné

Odborné a odovzdávacie miesta

Zavádzanie IMS

Zmena dodávateľa/BS

Typové diagramy

Namerané údaje

Merania OOM

Priebehové

Nepriebehové

Merania OOM výrobní

Priebehové

Nepriebehové

Merania hraničných OOM

Priebehové

Nepriebehové

Merania výrobní

Prehľad osobných údajov

Filter

Meno používateľa

Zobraziť

Filter tabuľky

Export

Excel

CSV

Existujúci používatelia

Neschválené požiadavky IMS

Strana 1 z 1

Počet zvolených záznamov: 0

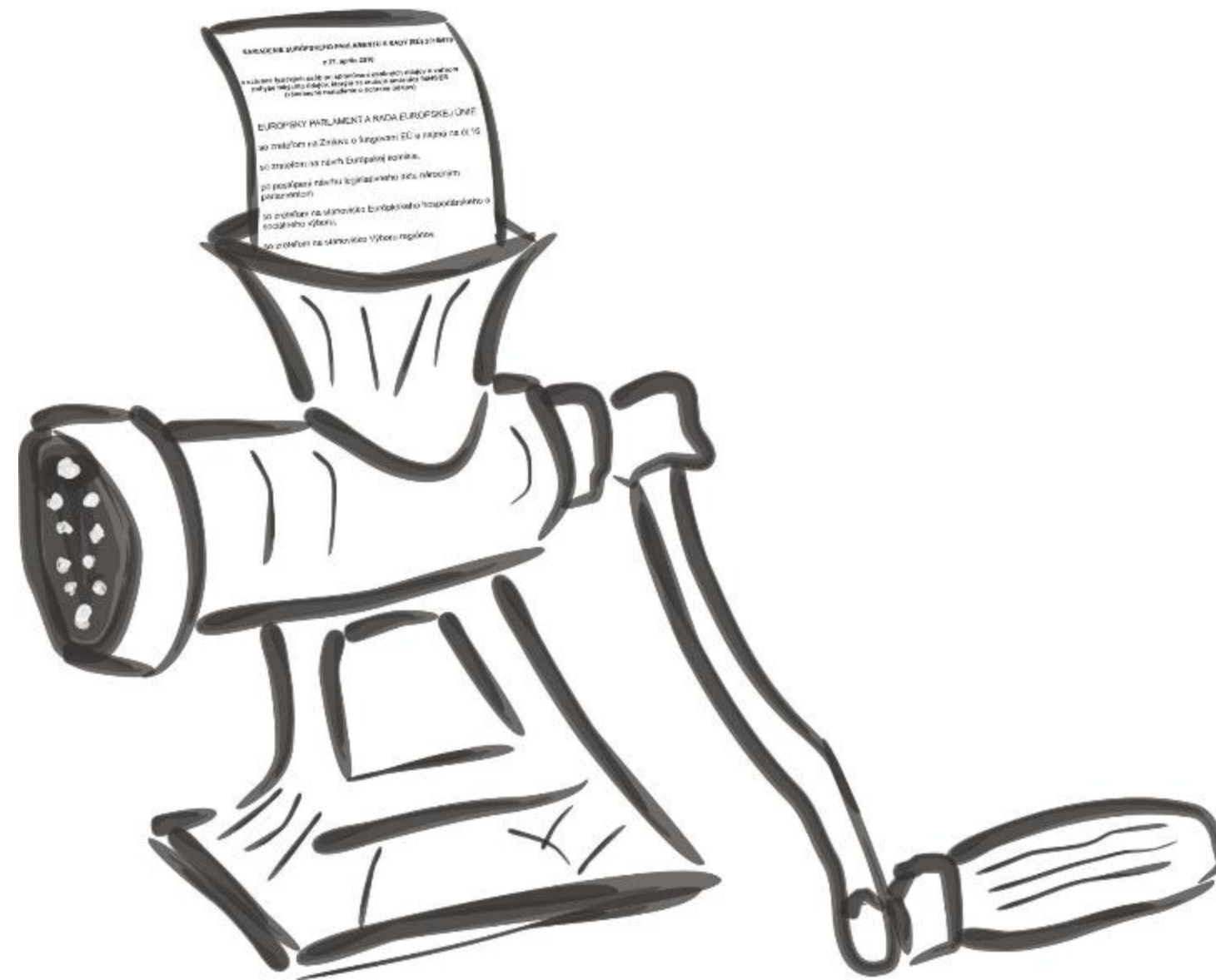
Uložiť nastavenia tabuľky

Zobrazujem 1 - 2 z 2

Copyright © 2017 [OKTE, a.s.](#)Design and Technology by [sféra, a.s.](#)

Postup implementácie

Súčasný stav pokrytia požiadaviek GDPR



- ✓ Identifikácia dotknutých systémov
 - ✓ Identifikácia OÚ v dotknutých systémoch
 - ✓ Analýza OÚ na základe ich spracúvania
 - ✓ Požiadavky GDPR pre prácu s OÚ
- Zabezpečenie povinností sprostredkovateľa

Postup implementácie

Zabezpečenie povinností sprostredkovateľa

GDPR:

- Zachovanie dôvernosti informácií
- Zaistenie technických a organizačných opatrení s cieľom zaistiť primeranú úroveň bezpečnosti
- Oznámenie prevádzkovateľovi po zistení porušenia ochrany OÚ

Náš prístup:

- Školenia oprávnených osôb, evidencia oprávnených osôb
- Zabezpečenie systémov, dvojfaktorová autorizácia, obmedzený a riadený prístup používateľov, zdokumentovanie interných procesov
- Zabezpečenie logovania prístupu používateľov k osobným údajom
- Heslovanie a šifrovanie citlivej komunikácie

Postup implementácie

Zabezpečenie povinností sprostredkovateľa

Logovanie prístupu používateľov k OÚ

- Potreba nástroja pre kontrolu a dohľadanie prístupu
- Nástroj musí poskytnúť odpoveď na otázku:

Kto, kedy, kde a k akým údajom pristupoval?

Šifrovanie citlivej komunikácie

- Medzi-systémová komunikácia zabezpečená cez HTTPS protokol
- HTTPS = hypertext transfer protocol **secure**

Šifrovanie citlivej komunikácie

- E-maily automatizovane odosielané zo systému (napr. faktúry, certifikáty)

Postup implementácie

Súčasný stav pokrytia požiadaviek GDPR



- ✓ Identifikácia dotknutých systémov
- ✓ Identifikácia OÚ v dotknutých systémoch
- ✓ Analýza OÚ na základe ich spracúvania
- ✓ Požiadavky GDPR pre prácu s OÚ
- ✓ Zabezpečenie povinností sprostredkovateľa

Čo máme ešte pred sebou

Záležitosti ktoré riešime alebo plánujeme riešiť



Automatizácia výmazu OÚ

Automatické „zmazanie“ osobných údajov v prípade zadania požiadavky na výmaz, ktoré bude zohľadňovať archivačné lehoty a potrebu údajov v systéme.



Zmena spôsobu zasielania údajov

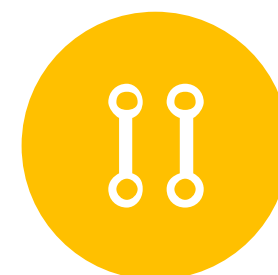
Najmä e-maily obsahujúce citlivé údaje:

- Faktúry,
- certifikáty e-ID



Implementácia logovania prístupu k OÚ

Potrebné nájsť vhodné riešenie naprieč všetkými IS.



Úprava zmlúv a dokumentácie

Ukotvenie súladu s GDPR do dôležitých dokumentov.



Šifrovanie komunikácie

Šifrovanie komunikácie medzi dodávateľmi elektriny a prevádzkovateľmi distribučných sústav

Čo nás dostalo do rozpakov

...t'žkosti, záhady...



Definícia osobných údajov

- Zamestnanci právnických subjektov

Používanie e-ID v občianskych preukazoch

- Akým spôsobom zasielať údaje

 Šifrovanie údajov na diskoch

- Je to primeraný krok?

 Úroveň riešenia GDPR

- Čo všetko pokryť v systémoch?
- Do akej miery ponúknuť automatizované riešenie?

Zhrnutie

Čo je podľa nás zmysel GDPR



Potreba vedieť kde všade sa nachádzajú osobné údaje

- Prehodnotenie umiestnenia údajov, prístupu k údajom



Potreba vedieť čo všetko sa deje s osobnými údajmi

Vznik -> spracovávanie -> zánik



Potreba zabezpečiť nové práva dotknutých osôb podľa GDPR

- Právo na zabudnutie
- Právo na prístup/prenositeľnosť



Potreba minimalizovať riziko zneužitia spracovávaných údajov – primerane

- Školenia pracovníkov, určenie zodpovednej osoby, interná dokumentácia
- Úpravy rozsahu spracovávaných údajov, úprava procesov, zmeny v systémoch



Byť aktívny v prípade narušenia ochrany osobných údajov

- Komunikácia s Úradom pre ochranu osobných údajov
- Komunikácia s dotknutými osobami



Karadžičova 2
811 08, Bratislava

Ing. Robert Maier
analytik



Robert.Maier@sfera.sk



0907 819 148



www.sfera.sk



Ďakujem za pozornosť
