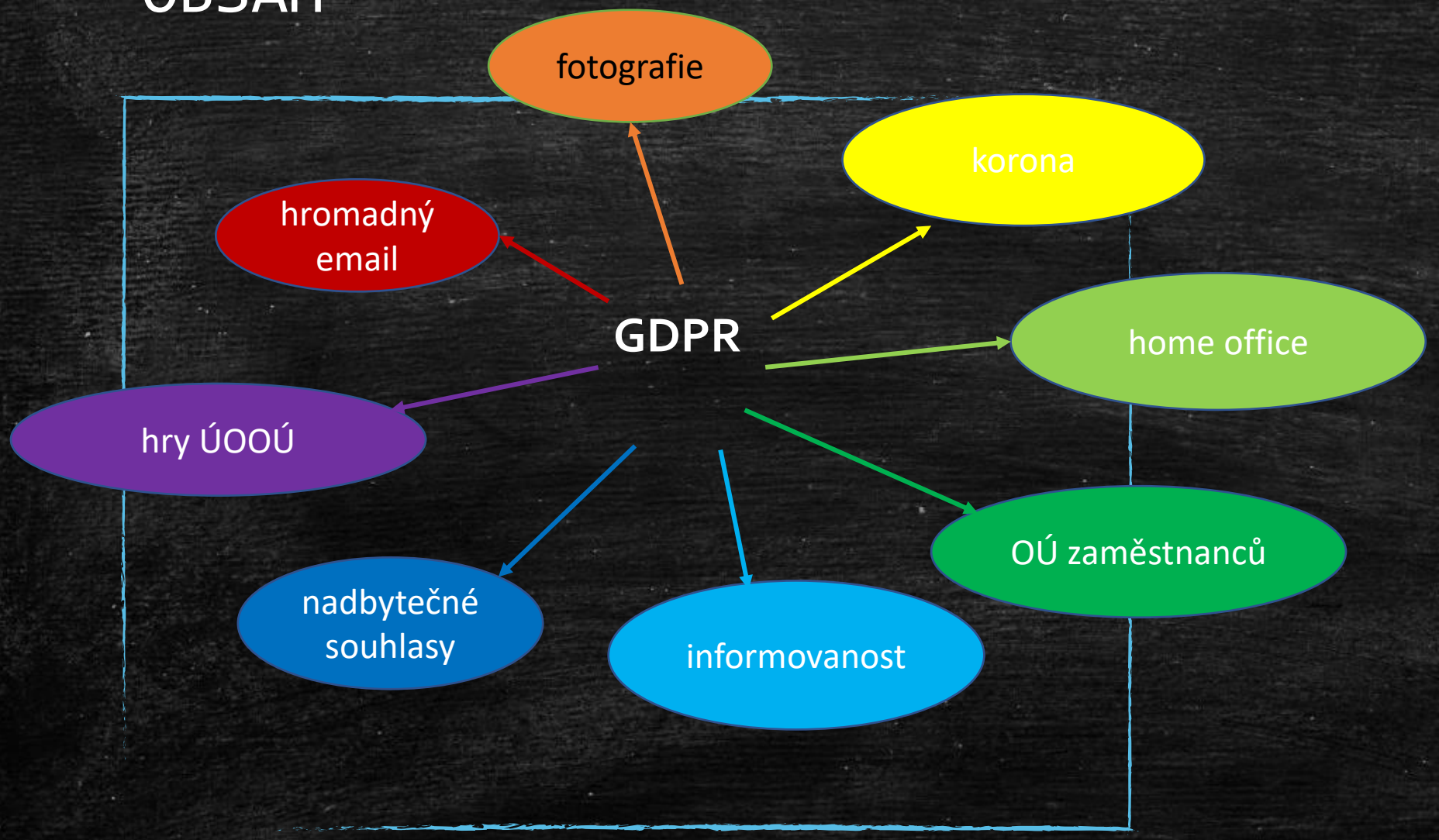
GDPR ve školním roce 2020/2021

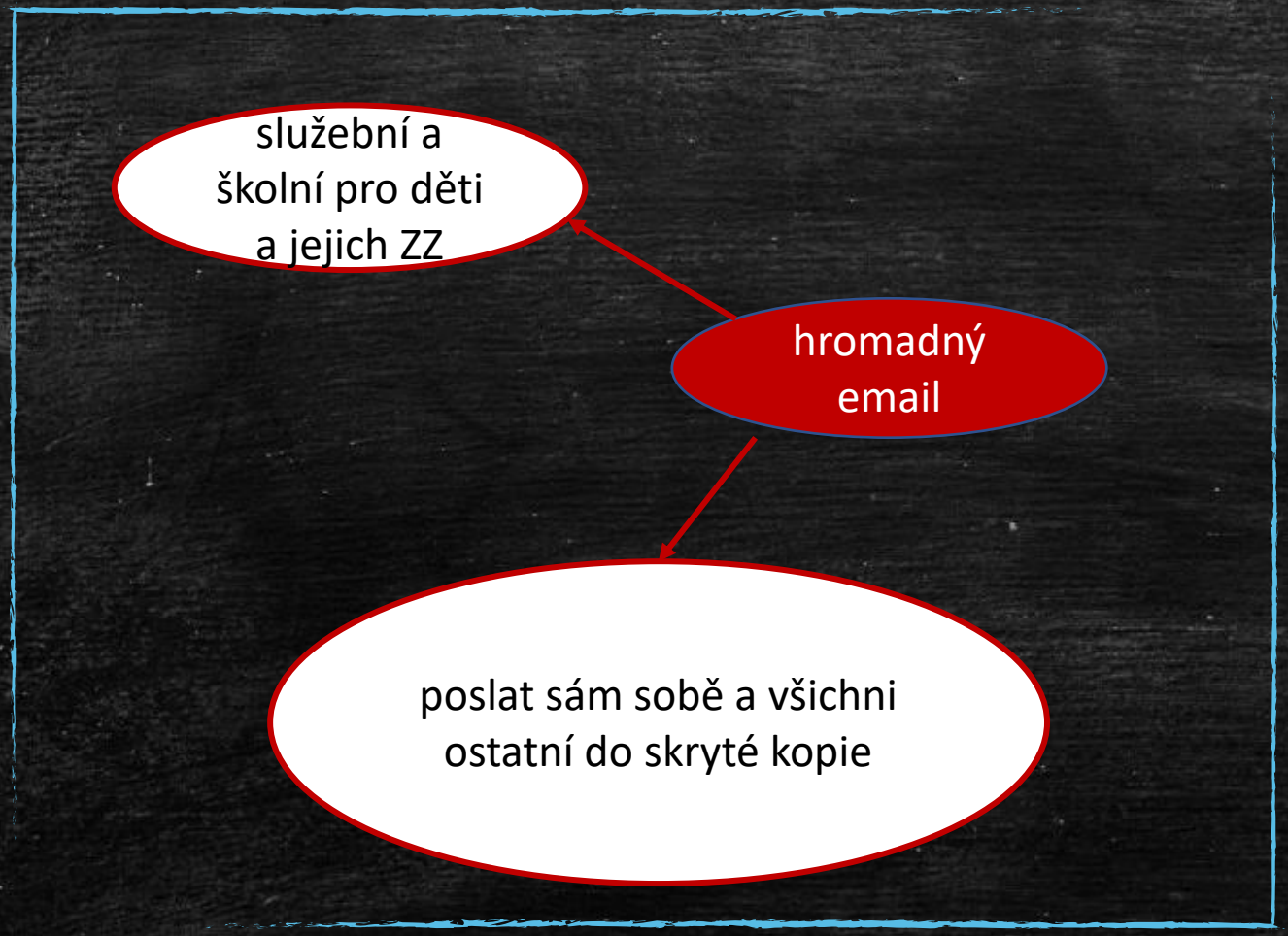
Ing. Hana Nidlová – pověřenec pro ochranu osobních údajů

GDPR

- General Data Protection Regulation

OBSAH


fotografie
korona
hromadný email
GDPR
home office
hry ÚOOÚ
OÚ zaměstnanců
nadbytečné souhlasy
informovanost


služební a
školní pro děti
a jejich ZZ
hromadný
email
poslat sám sobě a všichni
ostatní do skryté kopie

GDPR (obecné nařízení)

Poradna

- Často kladené otázky podle oblastí
  - K internetovým obchodům
  - Ke katastru nemovitostí
  - **K hromadným e-mailům**
  - Ze zdravotnictví
  - K pohledávkám a dluhům
  - K obcím a státní správě
  - Ze školství
  - K předávání osobních údajů do třetích zemí
  - K rodným číslům
  - K činnosti spolků, sportovních klubů a obdobných zájmových sdružení
  - Zaměstnavatelé
  - K vyžadování souhlasu
  - Ke kamerám a kamerovým systémům
  - K nevyžádaným obchodním sdělením a zákonu č. 480/2004 Sb.
- Mám dotaz. Jak postupovat?
- Chci podat stížnost na správce

K hromadným e-mailům

Sekce: Často kladené otázky

Je možné rozesílat hromadné e-maily s „otevřenou hlavičkou“?

Při odeslání e-mailu s „otevřenou hlavičkou“ (jednotliví adresáti vidí ostatní adresáty) dochází k předání osobních údajů jednotlivých adresátů, konkrétně jejich e-mailových adres spolu s informací, že jsou členy skupin, kterým jsou takové e-maily zasílány (například zákazníci určitého obchodu, členové určitého spolku apod.).

Mimo specifické situace, kdy je účelem hromadného e-mailu zahájení diskuze mezi jeho adresáty (otázka pořádání akce v rámci menšího spolku, kdy se všichni členové mají k této akci vyjádřit a kdy je zřejmé, že předání kontaktních údajů mezi členy tohoto spolku nepředstavuje žádné riziko pro subjekty údajů), by měly být všechny hromadné e-maily rozesílány tak, aby **ve zprávě nebyli viditelní ostatní adresáti**.

Kontext

Umístění: Složky dokumentů > Mapa stránek > Hlavní menu > Poradna > Často kladené otázky podle oblastí > K hromadným e-mailům

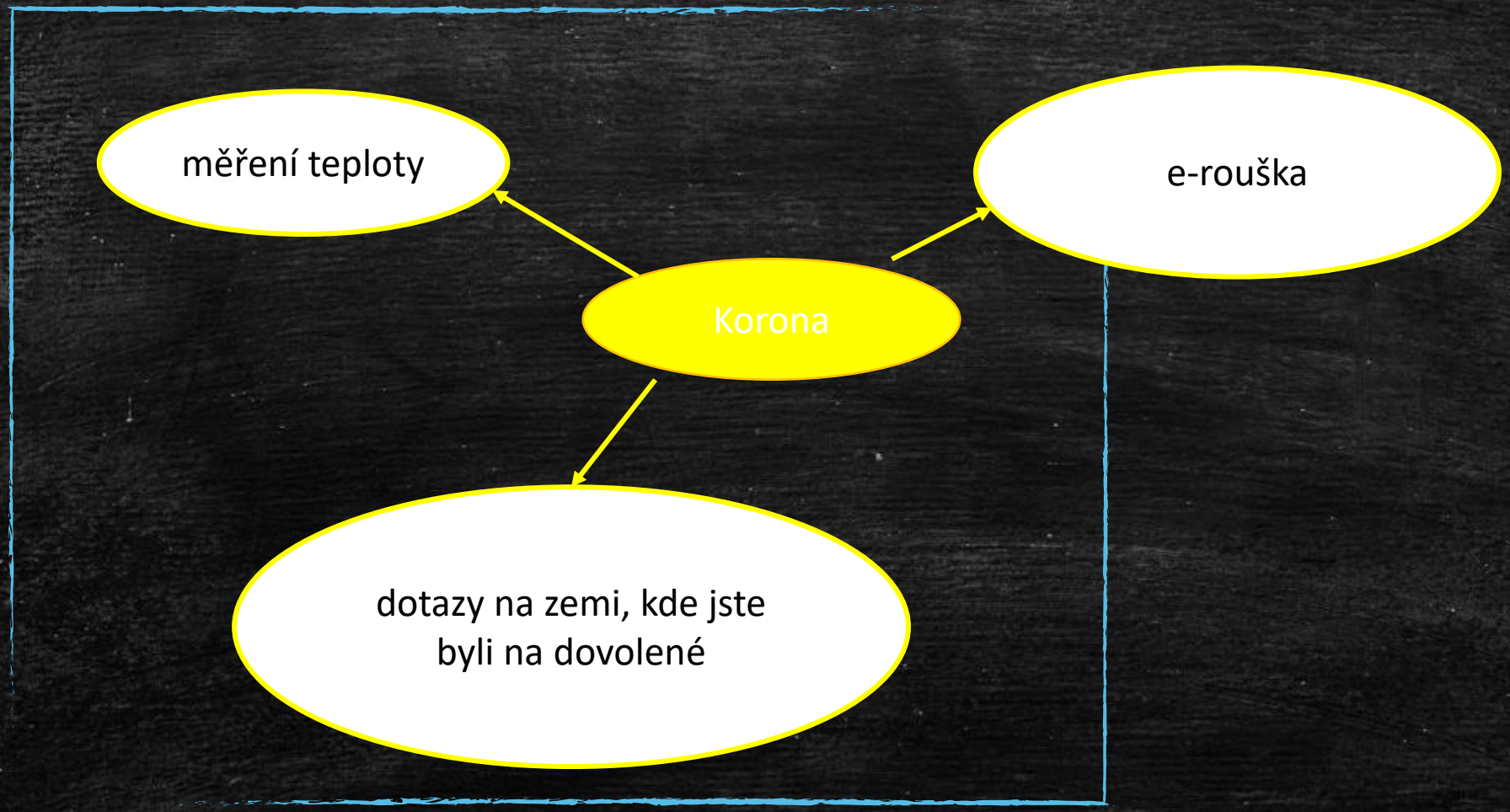
Zobrazit **aktuální dokumenty** | archiv dokumentů | dokumenty včetně archivu

beze jména na webu školy - NOZ

Fotografie

GDPR - se jménem na webu školy, bez jména na facebooku (profilování, severy mimo EU)

vždy informovat, že se na akci bude fotografovat


měření teploty
e-rouška
Korona
dotazy na zemi, kde jste
byli na dovolené

Může zaměstnavatel v současné situaci zjišťovat údaje o zdravotním stavu zaměstnanců např. při nástupu do práce?

Zákoník práce obecně ukládá zaměstnavateli povinnost vytvářet bezpečné a zdraví neohrožující pracovní prostředí a pracovní podmínky vhodnou organizací bezpečnosti a ochrany zdraví při práci a přijímáním opatření k předcházení rizikům.
V konkrétních situacích je zaměstnavatel povinen postupovat tak, aby **předcházel rizikům, odstraňoval je nebo minimalizoval**, mluví se o tzv. prevenční povinnosti. Zaměstnavatel je tedy v situaci ohrožení **povinen přijmout potřebná ochranná opatření odpovídající daným okolnostem**. Je přirozeně vhodné postupovat v součinnosti s orgány ochrany veřejného zdraví, kterým je také zaměstnavatel v některých situacích povinen ohlásit skutečnosti stanovené právní úpravou.
Zaměstnavatelé musí také v rámci preventivní povinnosti **informovat o rizicích vhodným způsobem ostatní zaměstnance**. Takové riziko může spočívat v tom, že na pracovišti se vyskytuje nebo vyskytovala nakažená osoba. Tehdy zaměstnavatel postupuje tak, že učiní veškerá nezbytná opatření. Skutečnosti o konkrétní osobě sděluje zaměstnavatel **pouze v rozsahu nezbytném k ochraně zdraví**, vždy tak aby nebyla dotčena důstojnost a integrita této osoby.

Může zaměstnavatel v souvislosti se svým oprávněným zájmem a zajištěním bezpečnosti na pracovišti během aktuální koronavirové situace požadovat, aby mu zaměstnanci sdělovali údaje o své dovolené? Tedy například kterou zemi navštívili, kde byli ubytováni, jak se stravovali či jakých hromadných akcí se zúčastnili?

Takto široce kladený okruh otázek porušuje zásadu minimalizace údajů. Je **nepřiměřený**.
Odpovídající jsou například formulace typu, zdali země, ve které zaměstnanec strávil dovolenou, není aktuálně na seznamu zemí označených jako rizikové, zda byly plněny požadavky orgánů ochrany veřejného zdraví z toho případně vyplývající či jestli si není vědom toho, že by přišel do styku s nákazou.
Zároveň je třeba dodržet **zásadu omezení uložení údajů na dobu nezbytně nutnou**. Není důvod, aby údaje týkající se možné nákazy byly zaměstnavatelem evidovány dlouhodobě.
V úvahu je třeba brát i charakter pracoviště.

Může zaměstnavatel uložit zaměstnancům povinnost používat aplikaci eRouška v pracovním (služebním) telefonu?

Aplikace eRouška je založena na dobrovolnosti. K jejímu používání **nemůže být nikdo nucen**, tedy ani zaměstnanec využívající služební mobilní telefon jako pracovní prostředek přidělený zaměstnavatelem. Zaměstnavatel nemůže bez zákonného zmocnění ukládat zaměstnanci povinnost stát se subjektem údajů ve zpracování, u kterého zaměstnavatel není správcem osobních údajů.
Povinné mobilní aplikace by ze zákona měly poskytnout záruky, že údaje umožňující identifikaci konkrétního uživatele aplikace jsou využity **pouze** k trasování možného šíření nákazy COVID-19, za důsledného dodržení zásady omezení uložení osobních údajů pouze po dobu nezbytně nutnou. K jinému účelu být využity nemohou.

home office

pozor na návštěvy i
rodinné příslušníky

Stanovisko č. 3/2014 - K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti

3_2014 [PDF, 232 kB]

srpen 2014[1]

Úvod

Jednou ze základních povinností správce je zpracovávat osobní údaje pouze na základě existence řádného právního titulu, jinak řečeno pouze v zákonem předvídané situaci, kdy lze údaje legálně zpracovávat. Výčet právních titulů pro zpracování osobních údajů je uveden v § 5 odst. 2 zákona č. 101/2000 Sb., pro zpracování citlivých údajů v § 9 téhož zákona. Samostatný právní titul pro zpracování osobních údajů za účelem zasílání nabídek obchodu nebo služeb je upraven v § 5 odst. 5 zákona č. 101/2000 Sb.

V obou uvedených výčtech možných právních titulů, tedy v § 5 odst. 2 a v § 9 zákona č. 101/2000 Sb. je jako první uveden (výslovný) souhlas dotčené osoby, subjektu údajů. Z této skutečnosti jsou v praxi nezřídka vyvozovány nepřesné závěry ústící ve vymáhání souhlasu se zpracováním osobních údajů i v případě, kdy je například toto zpracování správci uloženo zvláštním zákonem, a souhlas, či případný nesouhlas subjektu údajů, proto nehraje roli. Uvedený postup má za následek mimo jiné i nesprávné informování subjektu údajů o charakteru zpracování jeho údajů a tím nedostatečné plnění zákonné informační povinnosti ze strany správce. Nastíněnou otázkou se Úřad pro ochranu osobních údajů (dále jen „Úřad") částečně zabýval v jednom ze svých předchozích stanovisek,[2] nicméně pro vyjasnění se k této otázce vrací s detailnějším komentářem.

Základní právní úprava

V první řadě je nutno upozornit na skutečnost, že v doktríně ochrany osobních údajů má souhlas se zpracováním specifický význam. Není chápán jako integrální součást smlouvy podle § 5 odst. 2 písm. b) zákona č. 101/2000 Sb.

- GDPR (obecné nařízení)
- Právo na informace
- Poradna
- Pověřenec pro ochranu osobních údajů
- Povinně zveřejňované informace
- Právní předpisy
- Judikatura
- Dozorová a rozhodovací činnost
- Obchodní sdělení
- Zahraničí
- Schengen (informační systémy EU)
- Informační systém ORG
- Publikace
- Pro mládež

Hry

Hrát si, a ještě se u toho vzdělat. Ideální kombinace. Hry z této rubriky vám pomohou lépe pochopit základní principy ochrany osobních údajů. A ještě se skvěle pobavíte!

Rubriky

- **Interland**
  Hra od Googlu přináší hned čtyři napínavá dobrodružství se spoustou nástrah i legrace. A kromě získání úrovně "internetový Úžasňák" se ještě naučíte, jak si poradit s hackery, phishery, kyberšikanou nebo sdílením informací na sociálních sítích.
- **Digitální stopa**
  Jak je možné, že lidé, které jste nikdy neviděli, o vás mohou vědět úplně všechno? Projekt NÚKIB názorně ukazuje nejen to, jak málo stačí, aby se člověk stal obětí kyberšikany, ale dává také návod, jak z tohoto průšvihu ven.
- **Bad News**
  Autorem mezinárodně rozšířené hry o dezinformacích a jejich nebezpečí je nevládní organizace think-tank Evropské hodnoty. Zábavnou formou vás provede základními manipulačními technikami.
- **Než řekneš ano**
  Pomozte Sáře a Kristiánovi naplánovat včas svatbu a vyhnout se přitom některým internetovým nástrahám. Narazíte na bezpečnost přístupových hesel, nakupování v e-shopu, komunikaci na sociálních sítích, ale třeba také rychlé odstranění poškozujícího online obsahu, odhalení podvodného e-mailu či obranu proti kyberzločinu.
  Poučnou on-line hru pro vás připravily spotřebitelské organizace BEUC a dTest.
- **Cyber Chronix**
  Stáhněte si do telefonu aplikaci z dílny Evropské komise a pomozte hrdinům ze vzdálené planety překonávat překážky spojené s ochranou osobních dat.
- **Webowou diwočinou**
  Vytvořte si vlastní postavičku a projděte se úžasnou zemí fantazie. I zde vás však čekají nástrahy a úkoly ohledně ochrany vašich osobních údajů. Hru vytvořila Rada Evropy v rámci svého programu „Budujeme Evropu pro děti a s dětmi".

Rozbalit celý strom složek dokumentů

Dáváte fotky svých dětí na internet?

Rodiče, nechceme vás strašit, nechceme vás poučovat. Jen předkládáme fakta, která můžete sami zodpovědně zvážit. Někdo si to totiž třeba jen neuvědomí:
1. Nechtěný zájem o vaše dítě může vyvolat jedna jediná fotka umístěná veřejně kdekoli na síti.
2. Je to fotka před domem, ve vaší čtvrti, u školy, v kroužku? Dáváte tím světu na vědomí, kde se vaše dítě pravidelně pohybuje.
3. Tisíce lidí cíleně procházejí profily na sociálních sítích, internetová alba, videa, blogy a další webové stránky jen za tím účelem, aby našly "atraktivní" fotky či nahrávky dětí. Někteří se "jen" podělí o své úlovky na diskuzním fóru, jiní mohou mít touhu se s takovým dítětem setkat. Ti, kteří pouze předávají fotky, dostávají obsah k dalším. Nemáte šanci je nikdy poznat, stejně jako jejich motivace.
4. Myslete na to, že každá fotka, kterou jednou vložíte, žije na internetu navždy. Nikdy ji nesmažete. Nevíte, kdo ji má v počítači, komu ji pošle, na co ji použije a za jak dlouho ji může nechat opět vynořit.
5. Na takzvaném darknetu, tedy ve veřejnosti složitě přístupné části internetu, jsou fotky dětí z celého světa, ke kterým si pedofilové předávají důvěrné informace a vkládají sexuálně laděné komentáře.
6. Nejde zdaleka jen o to, jaké informace sami zveřejníte o svém dítěti. Internet je přece síť a v kombinaci s fotkami potenciálně velmi nebezpečná. Jaké informace jste zveřejnili o sobě, jaké jste publikovali vlastní fotky? Kolik snímků má škola na svém Facebooku či webu a kolik kamarádi vašeho dítěte? K těm se dá přece také snadno dostat: jsou to přátelé na Facebooku, sledující a sledovaní na Instagramu, komentující na Youtube. Vše se doplňuje a je to mozaika plná vodítek.
7. Zdaleka ne poslední bod, ale jeden z hlavních: Jaké přátele sami máte na sociálních sítích, kde zveřejňujete fotky potomků? Jste schopni se za všechny zaručit? A pokud jste přesvědčeni, že ano, víte, jak mají silná hesla? Víte, kdo s nimi v domácnosti používá počítač nebo jiné zařízení, přes které přistupují na sítě? Víte, že se nikde nezapomínají odhlásit?
Není nutné vidět za vším nebezpečí, je však potřeba dávat věci do souvislostí a používat kritické myšlení.
Doporučujeme k pročtení následující článek, zasazuje celý problém do reálného prostředí a vše dokresluje.

Ruský web pro pedofily vystavuje kradené fotky českých dětí

Na síti pro sdílení fotografií se objevují fotografie českých dětí ze stránek škol nebo ze sociálních sítí. Redaktoři Seznam Zprávy popisují, jak se tam dostaly.

Na začátku byly narozeniny, výlet na Sněžku, dovolená v plavkách a spousta fotek dvanáctiletého syna.
Všechny – a postupně jich bylo několik stovek – se Anna rozhodla uložit na největší českou sociální síť pro sdílení fotografií.
Jenomže snímky na internetu nezajímaly jen známé a příbuzné. Objevily se na ruském webu, na němž se sdružují pedofilové (redakce adresu zná, ale nezveřejňuje ji). A tak se Anna časem dozvěděla, že pod některými z nich by o synovi našla komentáře, které matce musí nahnat husí kůži.
„Je tak roztomilý s tím svým sladkým malým bříškem," zněl například jeden z nich.

Jdeme po nich

Že se dětské snímky sdílené v dobré víře na veřejném úložišti objeví i na ruském serveru pro potěchu pedofilů, zaskočí asi většinu matek.
Ještě víc by je mělo zaskočit, jak je ta cesta krátká a snadná.
Seznam Zprávy zjistily, že v případě Anny a jejího syna Matěje se o ni postaral muž vystupující v kyberprostoru pod přezdívkou XY.
Z úložiště, do něhož denně svěřují fotografie tisíce Čechů, stáhl Matějovy fotografie za několik posledních let a poté je prostě nahrál na zmíněnou ruskou síť.
Reportéři Seznamu přitom z internetu zjistili, že XY je aktivní, a tudíž poměrně nebezpečný. Nešíří totiž jen fotografie, ale také informace o dětech, které na nich jsou.
I když se snaží v kyberprostoru skrýt a na webu o sobě prozradí maximálně to, že by hranice oplotil ostnatým drátem a rád má svatomartinské víno, leccos o něm říkají jeho internetové debaty s pedofily.
XY na ruském webu krom Matějových snímků sdílel fotografie z dětských táborů a akcí skautu. Ostatním pedofilům doporučoval, aby si sami nějaké tábory našli, a doporučoval přímo stránky, kde je mohou objevit.
Z jeho komentářů k fotkám pak vyplývalo, že by děti mohl znát osobně, jelikož uváděl i detaily, které ze samotných fotografií rozhodně nebylo jednoduché vyčíst. Psal o osobnostech dětí, o jejich rodinách i o osobním zázemí. V některých komentářích dokonce bez okolků naznačoval, že s dětmi má určitý intimní poměr.
Je možné, že si informace vymýšlel, ale když redakce kontaktovala policii, dostala odpověď, že případy lidí podobných jako XY řeší.
„Policie se takovými případy zabývá," řekl pro Seznam Zprávy mluvčí Národní centrály pro boj s organizovaným zločinem Jaroslav Ibehej.

Děkuji za pozornost