

Posúdenie vplyvu podľa čl. 35 GDPR



Jakub Berthoty

Digital Legal, s.r.o.

21. septembra 2022

Aktuálne kybernetické hrozby, ako sa na ne pripraviť

DAGITAL LEGAL

O mne



Jakub Berthoty

Advokát a zakladateľ
Dagital Legal, s.r.o.

- Právne poradenstvo, **automatizované nástroje a vzdelávanie**;
- Služba **Data Protection Monitoring** zameraná na sledovanie noviniek, vývoj a vzdelávanie v oblasti;
- Pravidelné novinky cez náš www.dagital.sk/blog a [LinkedIn](#);
- O čom budem dnes hovoriť:

- **Historický vývoj**

- **DPIA:**

- Na čo má a nemá slúžiť DPIA?
- Čo musí obsahovať?
- Existujú vzory?
- **Náš prístup**

- **Príklady a ukážky z praxe**

Kontroverzná myšlienka na úvod:

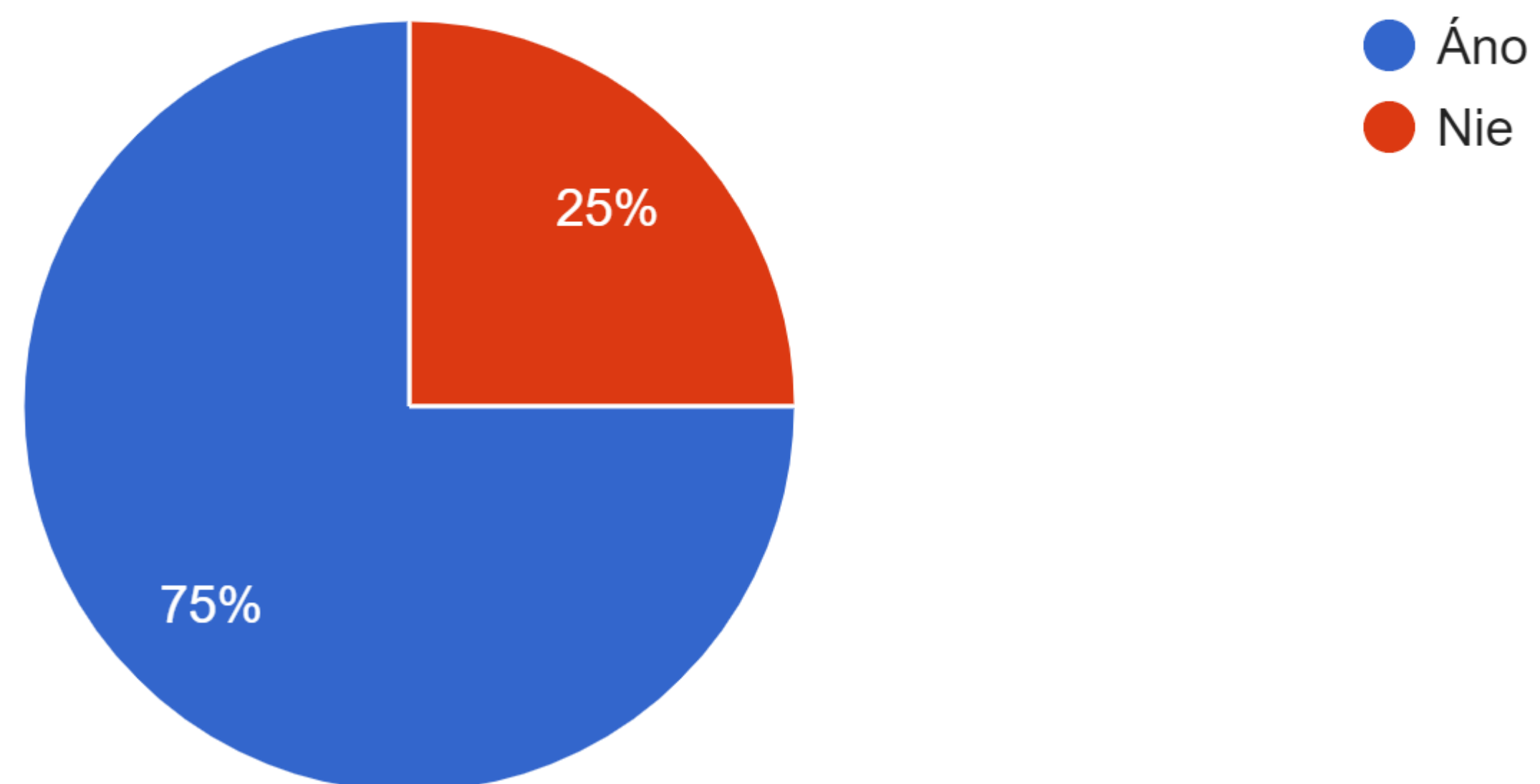
„Na Slovensku sme sa ešte nestretli s DPIA, ktoré by spĺňalo požiadavky čl. 35 GDPR...”

„Väčšina spoločností, ktoré majú vykonané DPIAs, v skutočnosti žiadne DPIAs nemajú.”



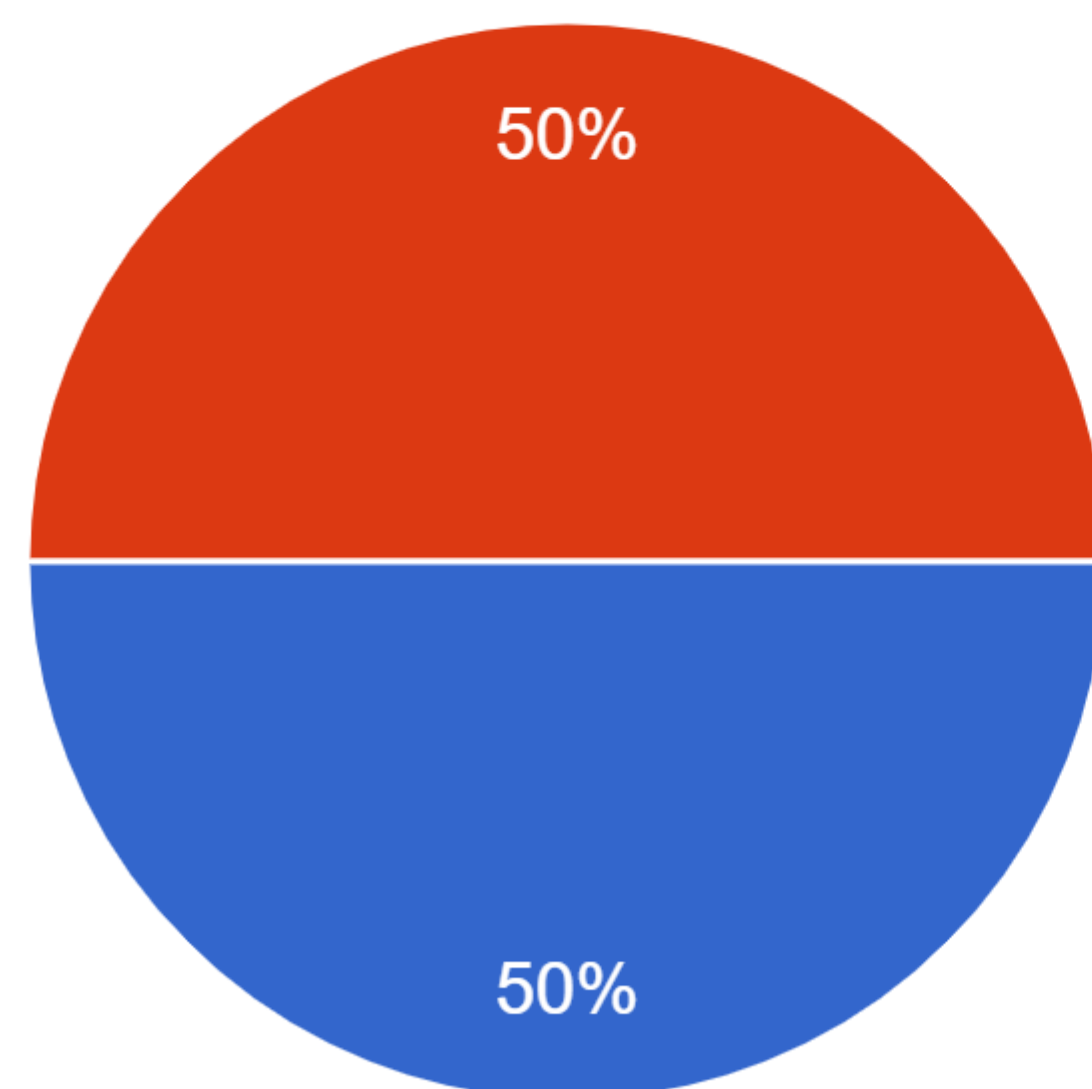
Vykonalí ste vo Vašej organizácii posúdenie vplyvu (DPIA) podľa čl. 35 GDPR?

16 odpovedí



Ak áno, vykonali ste posúdenia vplyvu

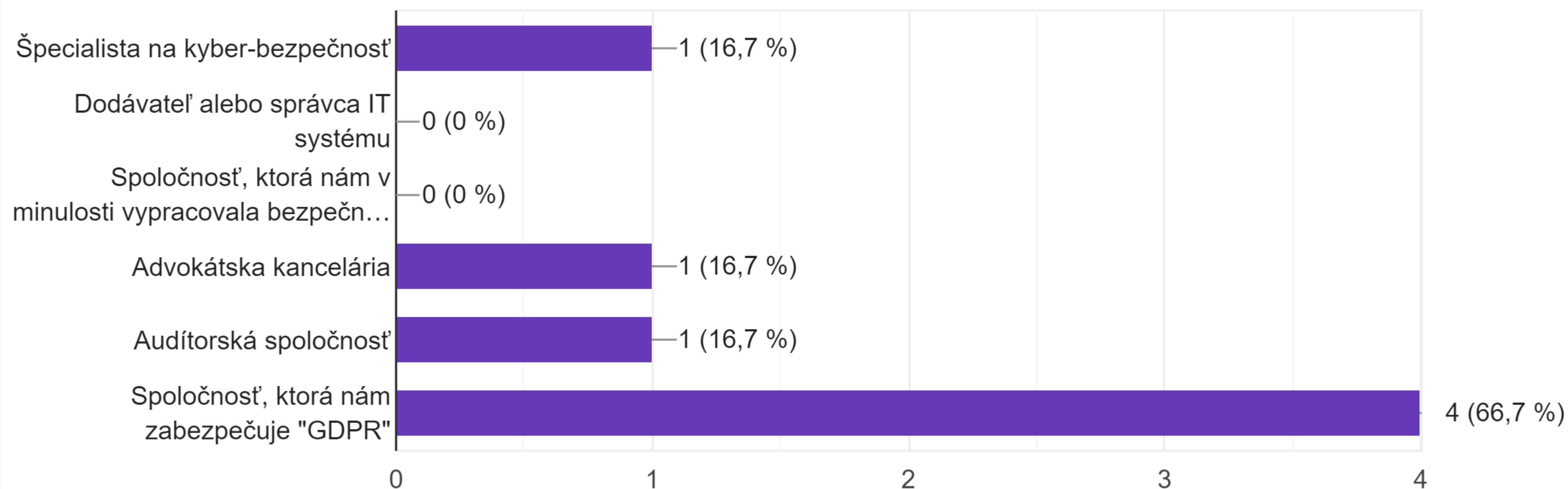
12 odpovedí



- Vlastnými kapacitami (interne)
- Prostredníctvom dodávateľa (externe)

Ak prostredníctvom externého dodávateľa, z akej oblasti pôsobenia bol tento dodávateľ

6 odpovedí



Historický vývoj



Dôležité míľniky

1. Od **14. apríla 2016** je známy text GDPR, ktorý definoval DPIA;
2. Dňa **4. apríla 2017** WP29 zverejnila prvé [„Guidelines k DPIA“](#) (ďalej len „**Usmernenia**“)
3. Od **25. mája 2018** je potrebné vykonávať DPIA, dovtedy taká povinnosť neexistovala (ani v Smernici 95/45/ES ani v SR);
4. Na historicky prvom zasadnutí Výboru dňa **25. mája 2018** Výboru prevzal Usmernenia (endorsed);
5. Prvá (žltá) publikácia ku GDPR na Slovensku vydaná v máji 2018;
6. Dňa **15. júna 2018** ÚOOÚ vydal [vyhlášku č. 158/2018 Z. z.](#) o postupe pri vydávaní posúdení vplyvu (ktorá sa však nevzťahuje na GDPR);
7. Dňa **11. júla 2018** požiadal ÚOOÚ o stanovisko k zoznamu spracovateľských operácií, ktoré podliehajú DPIA;
8. Druhá (oranžová) publikácia ku GDPR na Slovensku – **júl 2018**;
9. Dňa **25. septembra 2018** Výbor zverejnil [stanovisko č. 21/2018](#) k slovenskému zoznamu spracovateľských operácií;
10. Následne ÚOOÚ zverejnil slovenský zoznam spracovateľských operácií;
11. Tretia (modrá) publikácia ku GDPR vydaná v **októbri 2018**;
12. Úrad si začal pri takmer každej kontrole pýtať DPIA alebo odôvodnenie, prečo DPIA nepotrebuje.

Čo povedali ku DPIA tri múdre knihy

Valentová T. a kolektív (žltá kniha). GDPR, Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár. Bratislava: Wolters Kluwer SR, 2018, str. 224:

„DPIA nie je v podmienkach SR novinkou. DPIA bolo realizované úradom pri posudzovaní miery nebezpečenstva porušenia PS DO, ktoré realizovalo v rámci konania o osobitnej registrácii podľa zákona č. 122/2013. DPIA je komplex činností, ktoré sú súhrnom právnej analýzy vrátane analýzy dopadov na práva a slobody fyzických osôb.“

Hudecová, I. a kolektív (oranžová kniha), Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov / GDPR, Veľký komentár, Euro Kódex, Bratislava, 2018, str. 365:

„DPIA nie je ničím iným, než špeciálnym typom analýzy rizík. Niektoré organizácie majú nasadené procesy analýzy rizík už dávno, ako súčasť dobrej praxe príslušného odvetvia. DPIA však zohľadňuje subjektívny pohľad dotknutých osôb, naopak riadenie rizík v iných oblastiach (bezpečnosť informácií) je zamerané typicky na konkrétnu organizáciu.“

Berthoty, J. a kolektív (modrá kniha), Všeobecné nariadenie o ochrane osobných údajov. Praha: C.H. Beck, 2018, str. 320:

„DPIA je novodobý právny inštitút uvedený v čl. 35 GDPR. V predošlej európskej právnej úprave sa DPIA nevyskytuje, avšak to neplatí globálne. Jeho predchodcom je privacy impact assessment (PIA) – koncept, ktorý dodnes využívajú štáty ako Kanada, Francúzsko či Veľká Británia. Odlišujú sa však v tom, že DPIA dáva do popredia riziká pre dotknuté osoby a PIA sa zameriava na organizáciu a jej schopnosť chrániť údaje.“

** Pre čitateľnosť nie doslovné, ale prerozprávané referencie.*

Zhrnutie

Čo platilo v roku 2018:

1. Každý si pod DPIA predstavoval niečo trochu iné;
2. Každý si uvedomoval prepojenie na základné ľudské práva a slobody;
3. DPIA vypracovávali v organizáciách ľudia s úplne odlišnými skúsenosťami, zameraním a profesiami;
4. Výbor a dozorné orgány nezvládli a nestihli verejnosti vysvetliť, kedy sa má DPIA robiť;
5. Výbor a dozorné orgány nemali jasnú predstavu ani preferenciu, ako by DPIA malo vyzerieť;
6. Nebol zverejnený žiadny všeobecne uznávaný vzor / metodika k tomu, ako má DPIA vyzerieť.

Čo z týchto bodov platí aj v roku 2022?

- ***V podstate všetky;***
- ***S tým rozdielom, že viaceré autoritatívne DPIAs boli zverejnené a komunikované na verejnosť (v zahraničí).***

Samozrejme text GDPR a Usmernenia sa nezmenili...

Na čo má slúžiť DPIA?



Na čo má slúžiť DPIA?

Môj názor (nie text GDPR):

- Eliminovanie nepríjemných a nebezpečných situácií pre fyzické osoby, o ktorých spracúvame osobné údaje;
- Zabezpečenie ochrany ZLPS v typických, krajných a praktických životných situáciách, v ktorých sa môže Váš zákazník / zamestnanec ocitnúť v dôsledku nastavenia Vášho systému / produktu / spracúvania;
- Zohľadnenie širšieho kontextu spracúvania a spoločenskej zodpovednosti;
- Vyvažovanie stretu s akýmkoľvek inými právami a slobodami (prečo nie OP?).

Príklady:

- Možno keď Vaše dieťa bude cestovať samo lietadlom, budete chcieť aby letiská alebo letecké spoločnosti počítali s osobitným prístupom k právam a slobodám Vášho dieťaťa;
- Predstavme si klienta banky, ktorého anti-fraud systém odmietne autorizovať v nebezpečnej tretej krajine pri platbe kartou a klient zostane na čerpacej stanici bez zaplattenia. Hrozí mu a jeho rodine nebezpečenstvo života / zdravia?
- Predstavte si reklamu na antikoncepciu cielenú podľa histórie browsera a dopady zobrazenia takejto reklamy v domácnosti;
- Občan nemá aktivovanú e-schránku na www.slovensko.sk kde mu je doručený vymyslený exekučný titul a fikciou doručenia sa rozhodnutie stane právoplatné a jedného dňa mu exekútor príde zobrať dom, v ktorom býva.

Na čo nemá slúžiť DPIA?



Na čo nemá slúžiť DPIA?

- Na zabezpečenie primeranej úrovne bezpečnosti podľa čl. 32 GDPR;
- Samozrejme je tu prirodzený vzťah a DPIA môže prispievať z bezpečnosti, ale:
„Aj bezpečné spracúvanie bez narušenia integrity môže zabiť človeka.“ – ako?
- Bezpečnosť nie je primárnym / prvoradým cieľom DPIA – DPIA má ísť ďalej;
- Mimochodom, čo riešite v rovine analýzy rizík podľa čl. 32 GDPR ak obsahom posúdenia vplyvu sú riziká týkajúce sa napr. živelnnej pohromy, straty dát, hackerského útoku, požiaru a pod?
- DPIA nie je súčasťou ani oddielu 2 kapitoly IV GDPR s názvom „bezpečnosť osobných údajov“, tou je len čl. 32 až 34 GDPR;

Čo *musí* obsahovať *DPIA*?



Čo má DPIA obsahovať?

- **Základné náležitosti** definuje čl. 35 ods. 7 GDPR – tie musí obsahovať každá DPIA:
 - a. **systematický opis plánovaných spracovateľských operácií a účely spracúvania**, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ: jasne a zrozumiteľne opísať zamýšľaný postup spracúvania - prostriedky, spôsob uchovávania, kategórie príjemcov, dotknutých osôb alebo údajov, definovanie účelov,
 - b. **posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu; - v praxi veľký problém;**
 - c. **posúdenie rizika pre práva a slobody dotknutých osôb – hlavná časť DPIA**
 - d. **opatrenia na riešenie rizík** vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s GDPR, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka;
- **Ďalšie náležitosti** podľa čl. 35 ods. 8 a 9 GDPR – tie musí DPIA obsahovať iba niekedy:
 1. Posúdenie dodržiavania kódexov správania;
 2. Podľa potreby **názory dotknutých osôb/ich zástupcov** na zamýšľané spracúvanie bez toho, aby bola dotknutá ochrana obchodných alebo verejných záujmov alebo bezpečnosť spracovateľských operácií – **v praxi veľký problém.**
- **Ktoré ďalšie náležitosti DPIA nenájdete priamo v texte GDPR?**

Čo ďalšie by mala DPIA obsahovať?

- PRE-ASSESSMENT – ako Úradu preukážete, že DPIA nemusíte mať?
- EXPORT – ako vôbec zverejňovať a pracovať s celým DPIA bez ohrozenia záujmov spoločnosti / bezpečnosti?
- Katalóg všeobecne akceptovateľných rizík;
- Katalóg základných ľudských práv a slobôd;
- Ďalšie voliteľné opatrenia do budúcnosti (ešte neprijaté);
- Endorsement / podpis vedenia spoločnosti + dátumy?
- Aktualizácie každé tri roky? Ďalšie aktualizácie?
- História zmien – zásada zodpovednosti?
- Názor zodpovednej osoby?
- Metodika a proces DPIA – priamo súčasť dokumentu alebo súčasť interných predpisov?

Existujú vzory DPIA?



Najjednoduchší vzor (ICO) - [Britský dozorný orgán](#)



Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

DPIA template
20180622
v0.4

1

Step 1: Identify the need for a DPLA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

DPIA template
20180622
v0.4

2

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

DPIA template
20180622
v0.4

3

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

DPIA template
20180622
v0.4

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

DPIA template
20180622
v0.4

2

	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
--	------------------------------------	--------------------------------------	---------------------------

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Další velmi jednoduchý vzor - [IAPP](#)

Family Links Network
 Code of Conduct for Data Protection
 Template for Data Protection Impact Assessment (DPIA)

- Prior to conducting a DPIA, the following questions should be considered by National Societies:
- Have any consultations with internal stakeholders taken place with regard to risks arising from the processing operation and risks of non-compliance with the Code of Conduct?
 - Have any consultations with external stakeholders taken place? If yes, who, when and for what purpose?
 - In addition to identifying risks, have the consultations involved consideration of measures for avoiding or minimising the risks?

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
Purpose specification Is the data to be collected to be used only for a specified purpose? Will the data collected be used for anything other than the specified purpose?	2.1 Specified Purpose	Example: “Function creep” – National Societies may want to gain more value from the data they collect. In practice: National Societies may ignore or are not aware that they cannot repurpose personal data (i.e., to use the data they originally collected for some additional purposes) without seeking consent again. ➤ The National Society may not comply with the RFL Code of Conduct	Examples: ▪ Specify/document the purposes for which personal data will be collected/used ▪ Raise awareness on RFL Code of Conduct that provides for the purpose specification principle and for further processing only if for purposes compatible with the original purpose of data collection. ▪ Improve training of staff regarding purpose specification/compatible further processing. ▪ Use of database: As part of a privacy-by-design approach, insert reference in the file to ensure the purpose of the data	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
			processing operations is always specified. Where applicable, also link the purpose of the data processing operations to the consent that may have been provided.	
Data limitation Is all the personal data collected necessary for the RFL activity? When people engage with you seeking help, are they told how the personal information they supply will be used?	2.3.2 Processing adequate relevant and updated data 2.3.1 Responsibility and accountability 2.2.1 Consent 3.1 Information and access	Example: National Societies may collect more personal data than necessary for the specified purpose. In practice: National Societies may suffer reputational damage when it becomes publicly known that staff are collecting more personal data than they actually need. ➤ The additional personal data collected creates a bigger risk for the beneficiaries/ their families/witnesses/ or others if the system is hacked or otherwise compromised (unauthorized use/disclosure or security breach.) ➤ Collecting more detail than needed also	Examples: ▪ Ensure the staff collects only the pieces of data which are necessary to achieve the purpose specified originally ▪ If possible, give people prior notice regarding the modalities/purposes of the data collection and processing. Give individuals an opportunity to question the manner and purpose for which their data is collected and processed.	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

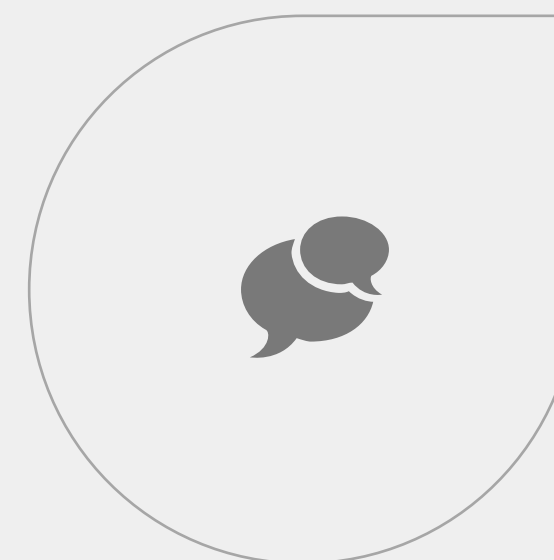
Ďalšie vzory, ktoré sú voľne dostupné:

- [Privacy International;](#)
- [Bristol University;](#)
- [Leeds;](#)
- [Witlshire;](#)
- [DPIA CCTV – UK GOV;](#)
- [ABGM;](#)
- [RCSI;](#)
- **Ale...**



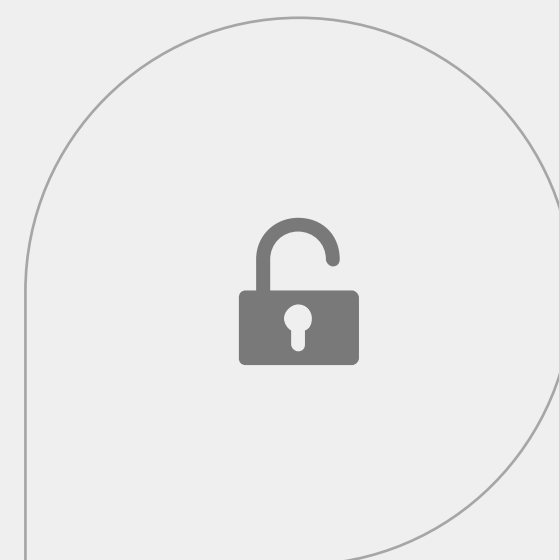
Náš prístup ku DPIA

Metodika + **interné predpisy** týkajúce sa DPIA



Diskusia s klientom a **samotná práca s /** vyplňanie DPIA

Autom. **Excel nástroj** na zachytenie obsahu a generovanie hodnotenia / výsledkov



Rôzne **export funkcie** v PDF formáte pre Úrad, verejnosť, manažment

Pre-assessment

Náš pre-asessment, ktorý podľa viacerých kritérií vyhodnotí, či:

- Je nutné vykonať DPIA;
 - Je skôr odporúčané vykonať DPIA;
 - Nie je potrebné vykonať DPIA.
-
- Všeobecné kritériá podľa čl. 35 GDPR;
 - Zohľadňuje aj zoznam situácií a kritérií podľa **Výboru a Úradu**;
 - Percentuálny výsledok + export.

Základné hodnotenie povinnosti vykonať posúdenie vplyvu		1 = Monitorovanie používateľov a zariadení	
Ide o systematické a rozsiahle hodnotenie osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu?	1 = Nie	Je nutné vykonať posúdenie vplyvu.	
Ide o spracúvanie osobitných kategórií údajov podľa článku 9 ods. 1 GDPR alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10 GDPR vo veľkom rozsahu?	1 = Nie		
Ide o systematické monitorovania verejne prístupných miest vo veľkom rozsahu?	1 = Nie		
Ide o operáciu, pre ktorú vyžaduje posúdenie vplyvu dotknutý dozorný orgán (napr. Úrad na ochranu osobných údajov SR)?	2 = Áno		
Otázka	Kritéria	Hodnotenie	Komentár
	Spracúvanie zahŕňa alebo nezahŕňa cezhraničné prenosy do tretích krajín nezarudujúcich primeranú úroveň ochrany?	1 = Nezahŕňa	
	Do spracúvania osobných údajov sú alebo nie sú zahrnuté tretie strany vôbec, t.j. Prevádzkovateľ ho vykonáva sám bez pomoci iných osôb?	2 = Sú zahrnuté	
	Prevádzkovateľ je alebo nie je v zmluvnom alebo inom obdobnom vzťahu s dotknutými osobami?	1 = Je	
	Aký je kontext plánovaného spracúvania?	1 = Môže očakávať	
	Môže dotknutá osoba primerane očakávať, že k danému spracúvaniu bude dochádzať?		
Aký je účel plánovaného spracúvania?	Ide o typický účel prevádzkovateľa?	1 = Áno	Ide o typický účel každého moderného podnikateľa.
Záverečné vyhodnotenie	Podľa odpovedí je odvodené odporúčanie pre každú sprac. operáciu.	Je nutné vykonať posúdenie vplyvu.	

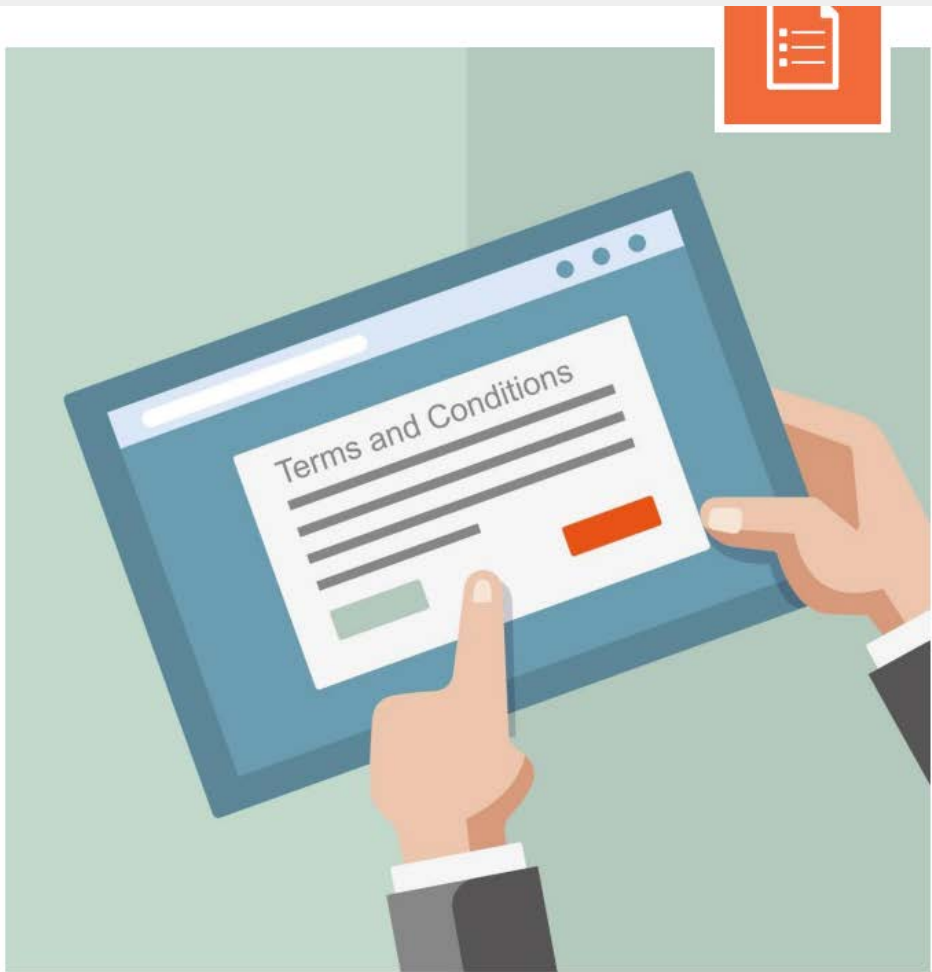
A	B	C	D	E	F	G	H	I	J	K	L
	HODNOTENIE	CELKOVO									
	1 = Silná autentizácia prístupov: vysoké riziko 2 = Vykonávanie automatizovaného individuálneho rozhodovania: vysoké riziko 3 = Bezpečnosť a vývoj IT: vysoké riziko	vysoké riziko	vyhodnotiť								
	Zašlite opisanie každej udalosti, ktorá by mohla mať za následok ohrozenie práva alebo slobody (min. 2)	Relevantní spracovateľská operácia (v každom prípade je potrebné vybrať viac)	Právomoc v dohovore o ochrane osobných údajov podľa práv a slobôd ("Dohovor")	Charita osobných údajov: Právomoc podľa Charty EÚ	Práva a slobody podľa Ústavy SR	GDPR práva dotknutých osôb	Vymaňovanie právnych základov: akékoľvek (prírodné) udalosti	Vysvetlenie existujúcich negatívnych dôsledkov udalosti na práva alebo slobody a ich hodnotenie	Odhad závažnosti udalosti a jej hodnotenie	Odhadovaná pravdepodobnosť udalosti a jej hodnotenie	Výsledok (č. 7)
	Udalosť	Spracovateľská operácia	Práva a slobody podľa EDEP	Práva a slobody podľa Charty EÚ	Práva a slobody podľa Ústavy SR	GDPR práva dotknutých osôb	Pôvod udalosti	Dôsledky	Odhadovaná závažnosť	Odhadovaná pravdepodobnosť	Posúdený vplyv
1		1 = Silná autentizácia prístupov 2 = Vykonávanie automatizovaného individuálneho rozhodovania	Právo na život (čl. 2 Dohovoru), Právo na slobodu a bezpečnosť (čl. 5 Dohovoru)	Právo na život (čl. 2 Charty), Právo na slobodu a bezpečnosť (čl. 6 Charty), Právo na ochranu osobných údajov (čl. 8 Charty)	Právo na život (čl. 15 Ústavy), Právo na ochranu zdravia (čl. 40 Ústavy)	Právo na vhodné technické a organizačné opatrenia (čl. 24-25 GDPR), Práva súvisiace s automatizovaným individuálnym rozhodovaním (čl. 22 GDPR)		3=Vysoko závažné dôsledky	3=Vysoká	2=Stredná	6

- WP 29: „Riziko je scenár, ktorý opisuje udalosť a jej následky odhadované v kategóriách závažnosti a pravdepodobnosti“
- Do posúdenia rizika však musíme dostať **aspekt základných práv a slobôd – ako?**
- **Aké práva a slobody**, podľa Dohovoru, Charty, Ústavy alebo GDPR?
- Prečo neprepojiť s konkrétnymi **spracovateľskými operáciami / účelmi**, ktoré vykonávame?
- Aby sme mohli v ďalšom kroku navrhovať opatrenia, **zaujíma nás pôvod udalosti**;
- Je na nás ako **kreatívne pristúpime k udalostiam**, ktoré sa rozhodneme v DPIA posudzovať – môže ísť o akúkoľvek udalosť;
- Samotné hodnotenie rizika – tu asi nič nové vymýšľať netreba...

Aké sú príklady z praxe?



Najznámejší zverejnený prípad DPIA – Nórsky úrad sa rozhodol nepoužívať ďalej Facebook.



Risk assessment: Should the Norwegian Data Protection Authority create a Page on Facebook?



Summary

The Data Protection Authority aims to increase awareness of and interest in privacy in Norway. In order to achieve this goal, we are considering establishing a presence on various communication platforms for effective communication with important target audiences. We consider Facebook to be well suited for several of the Authority's communication needs and ambitions.

The implementation of the General Data Protection Regulation (GDPR) in 2018 introduced new rights for citizens and new obligations for organizations. As a result of this new Regulation, both private companies and public authorities have had to review their procedures, practices and purchases involving the processing of personal data to ensure compliance with the new Regulation. The obligations imposed by the Regulation also apply when an organization uses social media, e.g. a Page on Facebook.

In this assessment, our capacity is neither that of a supervisory authority nor that of an ombudsman, but rather that of a data controller, with the obligations that follow from this role under the GDPR. Our assessment of Facebook is therefore primarily our organization's own assessment of what it would entail, in terms of accountability, to create a Page on Facebook, and of whether we would be compliant with relevant privacy laws.

In making sure the privacy of data subjects registered in a solution is protected, a Data Protection Impact Assessment (DPIA) is an important tool. This report addresses the risks and risk management associated with creating and communicating through a Page on Facebook. It presents a systematic description of the solution, a legal assessment of accountability, an assessment of the necessity and proportionality of processing, and considers measures to reduce privacy risks for the data subjects registered in the solution. The report also addresses ethical considerations in light of the Data Protection Authority's values¹ and the Authority's position as a role model in privacy issues.

¹ <https://www.datatilsynet.no/om-datatilsynet/planer/datatilsynets-strategi/>

Conclusion

This report was finalized by the Management Team. Based on this report and the recommendations of the Working Party, the Data Protection Authority has decided *not* to create and communicate through a Page on Facebook.

The Management Team agreed with the recommendations provided in the submitted report, with some amendments. This report includes changes based on discussions in Management Team meetings, as well as discussions in the organization's wider management meeting, including the final conclusion. The conclusion is based on an overall assessment, but has in particular emphasized the points below:

- The Working Party believes the risks to the data subjects' rights and freedoms associated with the processing of personal data through a Page on Facebook are too high.
- The Working Party believe that the Data Protection Authority will not be able to implement measures to satisfactorily mitigate these risks.
- The Working Party's assessment is that the Data Protection Authority would not be in compliance with Article 26 of the GDPR on joint controllers.
- The Working Party believes that it is not sufficient for The Data Protection Authority to enter into Facebook standard agreement with Facebook on joint controllership. The Data Protection Authority will not be able to establish a separate arrangement with Facebook.
- The Working Party's assessment is that it will probably not be possible for the Data Protection Authority to comply with the requirements of Article 25 of the GDPR on data protection by design and by default setting if we use Facebook.
- The Authority's data protection officer recommends that the Data Protection Authority not implement Facebook as a communication platform.

Necessity and proportionality of processing

We then assessed the processing and assured its necessity and proportionality. This has entailed assessing the legal basis for the processing, the protection of privacy principles and the rights and freedoms of users.

- The Data Protection Authority's legal basis for creating and using a Page on Facebook is derived from Article 6 (1) (f) of the GDPR on the balancing of interests. We believe we have several legitimate interests for being present on the platform, and that the processing would have several positive outcomes for the data subject.

The Working Party nevertheless believes that it is difficult to justify the Data Inspectorate's interests in using the Facebook page when these interests are weighed against the processing of personal data in Facebook.

- Regarding privacy considerations; we refer to the risks identified in the systematic description of the data processing. At the same time, we have emphasized considerations of a more ethical nature, such as the Data Protection Authority's own values, reputation and capacity as a role model for privacy. We have reason to believe there will be several different and conflicting views on processing, both within and outside the organization. We do not believe, however, that the processing will have a deterring effect on the population.

The Working Party also highlight some relevant considerations from a privacy perspective, as well as suggestions for measures for improving privacy terms and conditions:

- However, the Data Protection Authority would be at the mercy of Facebook and its terms and conditions by creating and using a Page on the platform. At the same time, we must be aware that Facebook can, at any time, amend these terms and conditions.
- The Working Party has identified some measures for improving privacy terms and conditions, and include transparency in the choice of communication platform, transparency in our assessments of the processing of personal data and of

controllership for this processing (Page on Facebook), as well as transparency of the practice of internal policies and moderations on the channel. We should also stay informed of any changes to Facebook's terms and conditions. In order to minimize data collection, no Facebook plug-ins or similar functionality would be implemented on our own website.

The Working Party have also made some assessments of processing in light of privacy principles and our impact on the data subjects' rights and freedoms:

The Data Protection Authority wishes all data processing taking place on a Facebook Page to be fair and respecting of the data subject's interests and reasonable expectations. Transparency about our internal policies on Page moderation and a dedicated contact person could contribute to this. Personal data collected by Facebook is used to make decisions about users and decisions that may affect users. It is uncertain how much personal data collected through the Data Protection Authority's Page on the platform would contribute to such decisions.

- The Working Party believe that the descriptions of the processing of personal data and considerations of accountability are characterized by a lack of transparency and clarification vis-à-vis Page owners and data subjects. After reading the documentation and attempting to prepare a complete systematic description of the data processing on the platform, there is still much we do not know about the processing. This is problematic from a privacy perspective.
- The Working Party believe the Data Protection Authority's own purposes have been clearly specified and correspond well with the expectations of users in the context of subscribing to and/or interacting with a Page on Facebook.
- The Working Party believe the Data Protection Authority's objectives, on their own, can be achieved by data minimisation; however, the platform does not permit that.
- The Working Party believe the principle of accuracy is less relevant in our context of

Assessment of risks to the data subjects' rights and freedoms

After considering the Authority's presence on a Facebook Page from the perspective of the Data Protection Authority being a data controller with a number of obligations pursuant to the GDPR, we flipped the perspective and considered the processing from the perspective of the data subject.

DPIA

Article 35 of the GDPR provides that a data protection impact assessment (DPIA) must be carried out when a certain type of processing is likely to result in a high risk to the rights and freedoms of the data subject under the Regulation.

Based on our findings from the systematic description in terms of the nature, scope, purpose and context of processing, and our conclusions in terms of necessity and proportionality, we have concluded that our use of Facebook as a communication platform would likely result in a high risk to the data subjects' rights and freedoms.

We also believe the processing fits several of the criteria of the Article 29 Working Party for evaluating when a DPIA is necessary¹⁰, as well as the Data Protection Authority's list of processing activities that always require a DPIA¹¹.

Assessment of co-determination, transparency and predictability

Our DPIA is based on the above criteria, and we assess *co-determination, transparency, predictability* in the processing, in accordance with the Data Protection Authority's own guide on data protection impact assessments. We do this to determine whether the processing can be performed in a manner that is acceptable and builds trust vis-à-vis the data subject.

Co-determination

We have assessed the degree of co-determination in light of the data subject's rights under the GDPR.

The Data Protection Authority and its data protection officer (DPO) can help the data subject to some degree by providing information and guidance in the exercise of

their rights within the Facebook system. However, the Data Protection Authority is largely unable to, in an active way, help the data subject exercise other rights.

Within Facebook, the data subject has the right and the freedom, beyond information about their data, to access (access), correct (rectification), transfer (data portability), and delete their own data. By law, data subject also has the right to oppose (object) and restrict certain types of processing of personal data. Among other things, this includes the right to object to the processing of data for direct marketing, the right to object to the processing of personal data where Facebook claims to be performing a task in the public interest or where Facebook is pursuing its own legitimate interest or the legitimate interest of a third party.

The data subject gives consent and is presented with the terms and conditions of the service when they create a profile on the platform. A user may withdraw their consent for certain types of processing on Facebook, such as the processing of special categories of personal data, the use of location data or the use of facial recognition. A user may at any time choose to delete their Facebook account.

The data subject may contact Facebook via a contact form, via mail or through a dedicated data protection officer with Facebook Ireland Ltd. The data subject may also file a complaint with Facebook Ireland's supervisory authority, the Irish Data Protection Commissioner, or through the Norwegian supervisory authority.

As we have already pointed out above, we believe there are uncertainties associated with the true opportunity to exercise several of these rights, e.g. the completeness of access to one's own data or a demand for permanent erasure of personal data. The nature of the platform means that a data subject would only, to a very limited degree, be able to exercise their rights vis-à-vis a specific Page on the platform. The data subject will, however, have some degree of choice in the platform's user functionality and interface.

Generally speaking, the Working Party believes that data subjects may have limited choice, limited options for reservations and limited true co-determination in a wide range of processing, including processing related to a specific Facebook Page, such as:

- Which types of personal data are collected, and the use of various sources.
- The volume of personal data.

¹⁰ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/yurdere-personvernkonsekvenser/yurdering-av-personvernkonsekvenser/?id=10362>

[personvernkonsekvenser/nar-ma-man-gjennomfore-en-yurdering-av-personvernkonsekvenser/](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/yurdere-personvernkonsekvenser/yurdering-av-personvernkonsekvenser/)

¹¹ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/yurdere-personvernkonsekvenser/yurdering-av-personvernkonsekvenser/>

Príklady z praxe (Data Protection Monitoring)

29

Pokuta cca 36 tisíc pre školu za používanie amerického vzdelávacieho systému



Islandský dozorný orgán uložil [pokutu](#) základnej škole, ktorá so súhlasom rodičov využívala vzdelávací systém založený na US cloude, pričom napr. dohoda o spracovaní údajov ani [DPIA](#) neboli dostatočné, chýbal účel spracovania, ale aj primeraná bezpečnosť údajov prenášaných do USA.

21

Biometrická kontrola zamestnancov si vyžaduje vykonanie DPIA



Španielsky dozorný orgán [pokarhal](#) stavebnú spoločnosť za implementáciu biometrického systému registrácie odtlačkov prstov na monitorovanie zamestnancov bez vykonania DPIA. Systém neukladal samotný obraz odtlačku prsta, ale hash a číselné hodnoty založené na odtlačku prsta v šablónach, ktoré registrovali fyzické vlastnosti a mohli sa použiť na individuálnu identifikáciu dotknutej osoby.

25

Pokuty takmer 10 miliónov eur pre dve telekomunikačné spoločnosti



Spoločnosti podľa gréckeho dozorného orgánu [neposkytovali](#) predplatiteľom jasné a dostatočné informácie, nekvalitne spracovali DPIA, neimplementovali adekvátne bezpečnostné opatrenia (napr. slabá anonymizácia). Zistenia nadväzovali na oznámenie o bezpečnostnom incidente.

41

Holandská vláda a univerzity zverejnili DPIA pre Microsoft produkty



Podľa [DPIA](#) Microsoft prijal opatrenia na nápravu vysokých rizík, ale organizácie by cloudové služby mali využívať na spracúvanie citlivých a špeciálnych kategórií údajov len ak môžu obsah zašifrovať pomocou vlastných šifrovacích kľúčov, a to aj potom, ako bude Microsoft uchovávať údaje v európskych dátových centrách.

25

Pokarhanie pre Frontex za prechod na cloud bez riadneho posúdenia ochrany údajov



EDPS [zistil](#), že Frontex prešiel do cloudu bez dostatočného posúdenia rizík ochrany údajov (DPIA) a bez vhodných zmierňujúcich opatrení alebo príslušných záruk na spracovanie. Frontex tiež nepreukázal, že zvolené riešenie (Microsoft 365) bolo výsledkom dôkladného posúdenia.

34

Francúzske ministerstvo nedostatočne implementovalo GDPR do aplikácie StopCovid



Podľa [rozhodnutia](#) napr. v zmluvách so sprostredkovateľmi chýbali náležitosti ako povinnosť pomáhať prevádzkovateľovi pri reakcii na žiadosti dotknutých osôb, v DPIA chýbali spracovateľské operácie ako anti-DDOS riešenie či využívanie technológie reCaptcha od spoločnosti Google.

03

Zoom v Holandsku zaviedol po vládnej DPIA množstvo dodatočných opatrení



[Výsledkom](#) DPIA je, že US spoločnosť vyriešila všetky známe vysoké riziká a uzavrela s holandskými orgánmi novú dohodu o spracovaní údajov. Keďže Zoom umožňuje šifrovať údaje pomocou súkromného kľúča, prenos údajov o obsahu do USA podľa prevádzkovateľov nie je vysokorizikový.

08

Stanovisko EDPB a EDPS k predĺženiu platnosti nariadenia o COVID certifikáte



Komisia plánuje predĺžiť platnosť nariadenia o digitálnom certifikáte COVID EÚ o 12 mesiacov a zmeniť niektoré jeho ustanovenia. EDPB a EDPS okrem iného negatívne [hodnotia](#), že nebolo vykonané DPIA a žiadajú, aby ho Komisia doplnila.

23

Pokuta takmer 7 tisíc eur za opomenutie konzultácie s dozorným orgánom



Dánsky dozorný orgán uložil [pokutu](#) stredisku, ktoré malo podľa výsledkov DPIA konzultovať s dozorným orgánom operácie, ktoré mohli predstavovať vysoké riziko pre práva dotknutých osôb, avšak pristúpilo k spracúvaniu bez predchádzajúcej konzultácie.

17

Univerzite bola uložená pokuta vo výške 200 tisíc eur za použitie „proctoring“ softvéru



Taliansky dozorný orgán uložil [pokutu](#) za využívanie kontrolného tzv. proctoring software, ktorý okrem iného monitoroval pohyby tváre študentov a ich okolie. Dotknuté osoby neboli dostatočne informované napr. o dobe uchovania údajov a prenose dát do USA, nepostačujúce bolo aj DPIA.

DPIA check-list na záver

1. Vieme našu DPIA alebo jej časť zverejniť tak, aby bola zrozumiteľná pre verejnosť?
2. Dá sa naša DPIA konzultovať s dotknutými osobami?
3. **Rieši naša DPIA skutočné životné situácie dotknutých osôb?**
4. Obsahuje naša DPIA všetky náležitosti podľa čl. 35 ods. 7 GDPR?
5. Vieme sa našou DPIA napríklad spýtať a reálne hodnotiť, či je v poriadku používať Facebook na cielenú reklamu?
6. **Vieme na základe našej DPIA prijímať business rozhodnutia?**
7. Obsahuje naša DPIA transparentný a objektívny bodovací systém?
8. Je možné našu DPIA použiť ako podklad pre dôvodovú správu alebo legislatívny proces prijímaného zákona?
9. Slúži nám reálne DPIA na niečo?

Ďakujem za pozornosť.

www.dagital.sk/cookies