ProLegis

Posúdenie vplyvu ochrany

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Právny rámec

1.1. General Data Protection Regulation (GDPR)

Článok 35

Posúdenie vplyvu na ochranu údajov

1. Ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie.

2. Prevádzkovateľ sa počas vykonávania posúdenia vplyvu na ochranu údajov radí so zodpovednou osobou, pokiaľ bola určená.

3. Posúdenie vplyvu na ochranu údajov uvedené v odseku 1 sa vyžaduje najmä v prípadoch:

(a) systematického a rozsiahleho hodnotenia 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,

(b) spracúvania vo veľkom rozsahu osobitných kategórií údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10, alebo

(c) systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

4. Dozorný orgán vypracuje a zverejní zoznam tých spracovateľských operácií, ktoré podliehajú požiadavke na posúdenie vplyvu na ochranu údajov podľa odseku 1. Dozorný orgán zasiela tieto zoznamy výboru uvedenému v článku 68.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Dozorný orgán môže stanoviť a zverejniť aj zoznam spracovateľských operácií, v prípade ktorých sa nevyžaduje posúdenie vplyvu na ochranu údajov. Dozorný orgán zasiela tieto zoznamy výboru.

6. Príslušný dozorný orgán pred prijatím zoznamov uvedených v odsekoch 4 a 5 uplatní mechanizmus konzistentnosti uvedený v článku 63, ak takéto zoznamy zahŕňajú spracovateľské činnosti, ktoré súvisia s ponukou tovaru alebo služieb dotknutým osobám alebo sledovaním ich správania vo viacerých členských štátoch, alebo ak môžu podstatne ovplyvniť voľný pohyb osobných údajov v rámci Únie.

7. Posúdenie obsahuje aspoň:

(a) systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,

(b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,

(c) posúdenie rizika pre práva a slobody dotknutých osôb uvedeného v odseku 1 a

(d) opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka.

8. Pri posudzovaní dosahu spracovateľských operácií vykonávaných relevantnými prevádzkovateľmi alebo sprostredkovateľmi sa náležite sleduje, či títo prevádzkovatelia alebo sprostredkovatelia dodržiavajú schválené kódexy správania uvedené v článku 40, a to najmä na účely posúdenia vplyvu na ochranu údajov.

9. Prevádzkovateľ sa podľa potreby usiluje získať názory dotknutých osôb alebo ich zástupcov na zamýšľané spracúvanie bez toho, aby bola dotknutá ochrana obchodných alebo verejných záujmov alebo bezpečnosť spracovateľských operácií.

10. Ak má spracúvanie podľa článku 6 ods. 1 písm. c) alebo e) právny základ v práve Únie alebo v práve členského štátu, ktorému prevádzkovateľ podlieha, a toto právo upravuje konkrétnu spracovateľskú operáciu alebo súbor daných operácií, a posúdenie vplyvu na ochranu údajov sa už vykonalo v rámci všeobecného posúdenia vplyvu v súvislosti s prijatím tohto právneho základu, odseky 1 až 7 sa neuplatňujú, pokiaľ členské štáty nepovažujú za potrebné vykonať takéto posúdenie pred začatím spracovateľských činností.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

11. V prípade potreby prevádzkovateľ vykoná prehodnotenie s cieľom posúdiť, či sa spracúvanie uskutočňuje v súlade s posúdením vplyvu na ochranu údajov, a to aspoň vtedy, keď došlo k zmene rizika, ktoré predstavujú spracovateľské operácie.

Recitály 89 do 96:

Článok 35 GDPR je úzko spojený s článkami 24, 25 a 32. Hlavným rozdielom medzi článkom 32 a článkom 35 je, že článok 32 (Bezpečnosť spracúvania údajov) sa zameriava na riziká spojené s nepriaznivými udalosťami, ako sú útoky, zatiaľ čo *Vplyv na ochranu osobných údajov* (DPIA), ktorý je založený na článku 35 sa **zameriava predovšetkým na riziká vyplývajúce z pravidelného spracovania údajov**.

DPIA je dôležitým nástrojom na zavádzanie ochrany údajov technologickými prostriedkami (ochrana údajov v štádiu návrhu), ako sa uvádza v článku 25 ods. 1. Oba sú založené na zásade predbežnej opatrnosti, tj identifikácii rizík už v počiatočných fázach návrhu, kde sa zvážia príslušné protiopatrenia pred zavedením a uvedením do prevádzky systémov spracovania údajov.

DPIA je nástroj na identifikáciu a analýzu týchto rizík. V prípadoch, keď nie je DPIA povinná, je potrebné vykonať analýzu súvisiacich rizík, aby sa primerane vykonávali ustanovenia článku 25 a článku 32. Obidve nariadenia sa výslovne týkajú práv a slobôd fyzických osôb. Hĺbka a požadovaná dokumentácia analýzy rizík, ktorá sa má vykonať, závisí od zložitosti a rizikovej miery spracovania. Odporúčame písomne predložiť dokumentáciu o analýze rizík. Implementácia princípu ochrany údajov podľa návrhu prekračuje riziká, ktoré boli vopred identifikované v najnovšej analýze rizík a obsahuje rozhodnutia, ktoré sa v neskoršom štádiu ad hoc realizovali vývojári systému (inžinierske systémy) pri vykonávaní zásad minimalizácie údajov.

2. Kedy sa vyžaduje DPIA[1]?

2.1. Základné informácie

DPIA sa musí vykonať pred spracovaním osobných údajov, ktoré nesú vysoké roziko práv a slobôd fyzických osôb.

V podstate sa DPIA musí vykonávať pre akúkoľvek formu spracovania údajov, ak sa nedá určiť a priori, že práva a sobody fyzických osôb nie sú ovpúlyvnené konkrétnou operáciou pre spracovanie údajov.

[1]Nasledujúci text sa významne zakladá na publikácii v nemeckom jazyku Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Pre aký typ spracovania údajov je potrebné takéto riziko predpokladať, napr. stanovených v bodoch uvedených v článku 35 ods. 3 alebo v odôvodnení 91. Dôraz sa kladie na používanie takzvaných nových technológií, vágneho právneho konceptu zavedeného v GDPR, pokiaľ ide o DPIA. Posúdenie rizika musí nielen zohľadniť existujúce rizikové konštelácie, ale aj pravdepodobnosť budúcich udalostí, ktoré sa majú identifikovať v prognostickom hodnotení. Výsledky hodnotenia musia byť zdokumentované..

Článok 35 ods. 1 posledná veta v spojení s odôvodnením 92 poskytuje dôležitý pohľad na posúdenie potreby DPIA: "Za určitých okolností môže byť primerané a ekonomicky vhodné, aby sa nepoužilo hodnotenie vplyvu na súkromie len na Ak chce verejné orgány alebo iné verejné orgány vytvoriť spoločnú platformu na aplikáciu alebo spracovanie, alebo keď viacero zúčastnených strán chce zaviesť spoločné aplikačné alebo spracovateľské prostredie pre celý podnikateľský sektor, na trhu segmentu alebo rozšírenej horizontálnej činnosti..

2.2. Prípady, v ktorých je DPIA povinná/záväzná

Čl. 35 Odd 3 obsahuje záväzné prípady použitia DPIA:

(a) systematické a rozsiahle hodnotenie osobných aspektov, ktoré sa týkajú fyzických osôb, a tie ktoré sú založené na automatizovanom spracovaní vrátane profilovania, a na ktorých sa zakladajú rozhodnutia, majúce právne účinky, ktoré sa týkajú fyzickej osoby,a lebo ktoré významne ovplyvňujú fyzickú osobu;

(b) spracovanie veľkého rozsahu osobitných kategórií údajov uvedených v článku 9 ods. 1 alebo osobných údajov týkajúcich sa odsúdení a trestných činov uvedených v článku 10; alebo

(c) systematické monitorovanie verejne prístupnej oblasti vo veľkom meradle.

2.2.1. Ďalšie úvahy týkajúce sa potreby realizovať DPIA

V odôvodnení 91 sa uvádzajú ďalšie prípady vyžadujúce DPIA:

Operácie spracovania

a) ktoré potenciálne zahŕňajú veľký počet ľudí a / alebo vysokú mieru rizika a / alebo využívanie rozsiahlej technológie v súlade s najnovšími technológiami;

b) ktoré zahŕňajú vysokú mieru rizika a sťažujú subjektom údajov, aby si uplatňovali svoje práva;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

c) ak sa osobné údaje spracovávajú pri prijímaní rozhodnutí o konkrétnych fyzických osobách po systematickom a rozsiahlom hodnotení osobných aspektov týkajúcich sa fyzických osôb na základe profilovania týchto údajov alebo po spracovaní osobitných kategórií osobných údajov, biometrických údajov alebo údajov o trestné odsúdenia a trestné činy alebo súvisiace bezpečnostné opatrenia;

d) ktoré predstavujú vysokú mieru rizika, pretože bránia dotknutým osobám vo výkone práva alebo využívania služby alebo plnenia zmluvy;

e) ktoré predstavujú vysoké riziko, pretože obsahujú systematický veľký rozsah

2.2.2. Vykonávanie DPIA pre niekoľko podobných systémov na spracovanie údajov

V článku 35 ods. 1 sa uvádza, že pre systémy spracovania s podobnou úrovňou rizika sa môže vykonať jednotná DPIA. Pri posudzovaní takejto podobnosti sa musí zvážiť celkový účel spracovania údajov v každom jednotlivom prípade. V odôvodnení 92 sa uvádza, že vzhľadom na hospodárske náklady môže mať DPIA širší tematický rozsah, vďaka čomu majú členovia v konkrétnom odvetví alebo v segmente trhu možnosť pokryť aplikácie alebo spracovateľské prostredie alebo široko zdieľané horizontálne postupy s jediným DPIA.

2.2.3. Pozitívne a negatívne zoznamy DPIA

Možno predpokladať, že regulačné agentúry zverejnia pozitívne / negatívne zoznamy, ktoré povedú k rozhodnutiu, či sa v konkrétnom prípade vyžaduje DPIA. Tieto zoznamy definujú typy spracovania vyžadujúce DPIA ("pozitívne zoznamy") a prípady, keď sa nevyžaduje DPIA ("negatívne zoznamy"). Obidva zoznamy musia národné regulačné orgány zasielať Európskej rade pre ochranu údajov ako súčasti režimu regulačnej súdržnosti (článok 35 ods. 4) s cieľom zabezpečiť lepšiu harmonizáciu v celej EÚ.

Treba poznamenať, že pracovná skupina zriadená podľa článku 29 (WP/PS29) odporúča vykonať DPIA aj v prípadoch, kde sa zdá byť nejasné, či je potrebné, aby sa DPIA prispelo k splneniu právnych požiadaviek na riadnu ochranu údajov.

2.3. Načasovanie DPIA

Načasovanie a metóda, ktoré sa uplatňujú na DPIA, stanovuje správca. Predpokladajú sa právne sankcie v prípade nevykonania DPIA. Odporúča sa začať prípravu na DPIA v najskoršom možnom štádiu projektu. Každé oddelenie alebo príslušní zamestnanci, ktorí sa podieľajú na spracovaní údajov, musia iniciovať príslušné procesy. Školenie sa odporúča preto, aby sa zvýšila informovanosť o potrebe DPIA v rámci organizácie

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Zváženie opatrení na minimalizáciu rizika v počiatočnom štádiu akéhokoľvek projektu vrátane spracovania údajov, môže pomôcť udržať byrokratické úsilie na pomerne nízkej úrovni.

DPIA môže usmerňovať vyhľadávanie adekvátnych riešení a môže pomôcť implementovať - ako už bolo spomenuté vyššie - požiadavky na ochranu údajov efektívne a včas prostredníctvom vhodných technologických riešení (ochrana údajov podľa návrhu) a výberu predvolených nastavení s ohľadom na ochranu údajov.

Za predpokladu komplexných a intenzívnych príprav DPIA bude usmerňovať plánovaný projekt od fázy skorých nápadov až po jeho konečné operatívne vykonávanie a preukáže iterakčný charakter procesu DPIA.

Či sa DPIA požadovalo pre spracovanie činností, ktoré boli účinné pred všeobecnou platnosťou GDPR (25. mája 2018), je otvorená otázka. Prijatím doslovného znenia ("pred") sa vyžaduje DPIA len pre procesy, ktoré začali fungovať po 25. máji 2018 alebo ktoré po tomto dátume prechádzajú značnými zmenami..

Keďže v týchto prípadoch systém spracovania údajov už funguje, predbežná kontrola nie je možná. Okrem toho tieto operácie neexistujú v neregulovanom priestore (za predpokladu, že boli zohľadnené všetky právne predpisy a požiadavky na podávanie správ z predchádzajúceho právneho rámca).

Napriek tomu PS/WP29 dôrazne odporúča formu DPIA pre spracovateľské systémy, ktoré sa už používajú, aby sa predišlo právnej neistote a dokonca aj právnym sankciám.

2.4. Posúdenie DPIA

Po vykonaní DPIA je potrebné vykonať aj reviziu-prehodnotenie navrhovaných opatrení, ak sa to považuje za potrebné. Možno považovať za nevyhnutné preskúmanie samotného spracovania údajov na identifikáciu akýchkoľvek nových prvkov rizík súvisiacich so spracovaním údajov. V odôvodnení 89 sa uvádza, že po prvom posúdení môže byť potrebná revízia DPIA v primeranom čase. Pri vykonávaní protokolu DPIA by mal byť súčasťou dokumentácie časový rámec pre rutinné kontroly alebo budúce obnovy.

Treba zvážiť technologický vývoj, novú právnu úpravu a zmeny v spracovateľských postupoch. Ak dôjde k riziku, musí sa uzavrieť nová zmluva DPIA.

Povinnosť vykonávať DPIA je súčasťou povinnosti kontrolóra údajov, ktorý dokumentuje ich zodpovednosť. Dokumentácia a správa by nemali poskytovať iba informácie o vykonávanom DPIA, ale mali by uvádzať všetky dôvody, prečo nebolo predprípravu

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

kompletného DPIA, alebo ukončenia DPIA po zistení vysokých rizík vzhľadom na dotknuté osoby.

2.5. Konzultácia s orgánom na ochranu osobných údajov podľa Čl. 36 GDPR

Prevádzkovateľ uskutoční s dozorným orgánom pred spracúvaním konzultácie (DPA), ak by DPIA odhalila závažné riziká a prevádzkovateľ by nevedel, ako prijať akékoľvek nápravné opatrenia na zmiernenie takýchto rizík. DPA musí reagovať na túto žiadosť o konzultáciu do štrnástich týždňov. Pri komplexných a inovatívnych projektoch sa odporúča začať DPIA v najskoršom možnom štádiu, takže akékoľvek odporúčania DPIA môžu byť zohľadnené pri realizácii plánu projektu.

3. Kto zodpovedá za riadenie DPIA?

3.1. Základné informácie

Zodpovednosť za vykonávanie smernice DPIA je v právomoci prevádzkovateľa - v tomto prípade je to miestny verejný orgán. Najprv návrh Komisie prevzal/presunul zodpovednosť za DPIA spracovateľovi údajov, ktorý koná podľa príkazu prevádzkovateľa. Naopak, odôvodnenie 95 sa obmedzuje na nárok na spracovateľa, aby pomohol správcovi, ak je to potrebné a na požiadanie, pri zabezpečovaní dodržiavania povinností, ktoré vyplývajú z posúdenia vplyvu ochrany údajov.

V praxi bude vhodné zmluvne požadovať, aby bol spracovateľ, ktorý je k dispozícii, aby bol zapojený do aktívnej podpory počas celého procesu DPIA. Toto je tiež nad rámec článku 28 ods. 3 písm. F), v ktorom sa ustanovuje, že zmluva o spracovaní (alebo iný právny nástroj) by mala poskytnúť spracovateľovi, berúc do úvahy povahu spracovania aj informácie, ktoré má k dispozícii, dodržiavanie povinností vyplývajúcich z článkov 32 až 36. Často iba spracovateľ disponuje potrebnými informáciami na posúdenie príslušných aspektov spracovania. Pritom sa musí brať do úvahy riziko zverejnenia obchodných a obchodných tajomstiev. Opäť sa odporúča konkrétne zmluvné nariadenie. Ak sa predpokladá spracovanie údajov spoločnými kontrolórmi, DPIA v zmysle čl. 35, ods. 1, ods. 2, môže byť vykonané aj jedným z riadiacich jednotiek - ktorý nevypúšťa ostatných zodpovedných kontrolórov

3.2. Účasť v DPIA

DPIA by sa mal organizovať ako projekt a ako taký by mal byť vybavený potrebnými materiálnymi a ľudskými zdrojmi zodpovedajúcim vysokým stupňom riadenia. Pri zostavovaní projektového tímu je potrebné venovať osobitnú pozornosť komplexnosti

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

projektu, požadovaným odborným znalostiam a potrebným znalostiam o konkrétnom projekte a jeho prostredí. V praxi môže byť vytvorený tím právnikov, IT pracovníkov, CISO, úradník pre ochranu údajov, oddelenie, ktoré požiadalo o spracovanie ("vlastník údajov") atď.

Osobitná pozornosť sa venuje zabezpečeniu a forme predchádzania konfliktom záujmov. Tí, ktorí sa v budúcnosti zaoberajú spracovaním údajov, sa nemusia považovať za nezávislých, ale na druhej strane môžu poskytnúť cenný prínos pre vypracovanie hodnotenia vplyvu na súkromie. Implementáciu môže vykonávať interný tím, ako aj externé tretie strany. V ideálnom prípade by mal byť zapojený aj nezávislý orgán.

Kontrolór sa musí poradiť s úradníkom pre ochranu údajov. V súlade s článkom 39 ods. 1 písm. C) poradenstvo, ktoré sa týka DPIA a monitoruje sa vykon, ktorý patrí medzi zákonné povinnosti DPO, avšak len na požiadanie a nie na pre tých na vedúcej pozícii.

Preto je povinnosťou kontrolóra získať poradenstvo úradníka pre ochranu údajov. V akej dobe a do akej miery musí byť pracovník ochrany údajov zapojený do procesu, je to na rozhodnutí správcu. Následné preskúmanie záverečnej správy by bolo postačujúce. V praxi sa dôrazne odporúča včas zapojiť úradníka pre ochranu údajov, hlavne kvôli jeho odbornosti.

V závislosti od organizácie kontrolóra je vhodné, aby bola DPIA schválená na úrovni riadenia alebo zodpovedajúcim autorizovaným orgánom.

4. Ako zaobchádzať s DPIA

4.1. Základné informácie

x 1. Je potrebné zdôrazniť, že GDPR nepredpisuje žiadnu konkrétnu formu ani konkrétnu metódu navrhovania hodnotenia vplyvu na ochranu údajov, o ktorej sa v súčasnosti intenzívne diskutuje na vnútroštátnej a európskej úrovni. WP29 uvádza, že na podporu implementácie ustanovení GDPR možno použiť rôzne možnosti návrhu a odkazuje na príklady existujúcich modelov procesov DPIA (všeobecných alebo sektorových) v prílohe 1.[2]

2 WP29, WP 248, 15: Different methodologies (see Annex 1 of WP248 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR (Annex 1).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.2. Implementácia DPIA

Prevádzkovateľ je v podstate slobodný v tom, ako má vykonávať proces DPIA a môže ho prispôsobiť existujúcim vnútorným postupom za predpokladu, že miestna verejná autorita/orgán zohľadní štyri požiadavky uvedené v článku 35 ods. 7 smernice GDPR a) d) ako minimálne požiadavky DPIA, ktoré podrobnejšie opisuje pracovná skupina zriadená podľa článku 29 a okrem toho berie do úvahy bod "zainteresované strany" (pozri článok 35 ods. 2) a názory dotknutých osôb [pozri článok 35 ods. 9]):

a) systematický opis zamýšľaných spracovateľských operácií a účel spracovania vrátane prípadného oprávneného záujmu kontrolóra;

b) posúdenie nevyhnutnosti a proporcionality spracovateľských operácií vo vzťahu k účelom;

c) posúdenie rizík týkajúcich sa práv a slobôd dotknutých osôb uvedených v odseku 1; a

d) opatrenia plánované na riešenie rizík vrátane bezpečnostných opatrení, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením s prihliadnutím na práva a oprávnené záujmy dotknutých osôb a iných dotknutých osôb.

4.3. Minimálny obsah DPIA

Článok 35 ods. 7 písm. A) až d) GDPR v súvislosti s odôvodneniami 84 a 90 vyžaduje minimálne:

a) systematický opis zamýšľaných spracovateľských operácií a účel spracovania vrátane prípadného oprávneného záujmu kontrolóra;

b) posúdenie nevyhnutnosti a proporcionality spracovateľských operácií vo vzťahu k účelom;

c) posúdenie rizík týkajúcich sa práv a slobôd dotknutých osôb uvedených v odseku 1; a

d) opatrenia plánované na riešenie rizík vrátane bezpečnostných opatrení, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením s prihliadnutím na práva a oprávnené záujmy dotknutých osôb a iných dotknutých osôb.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Písmená c) a d) sú prejavmi tzv. "Prístupu založeného na riziku" GDPR, ktoré sú relevantné nielen pri implementácii DPIA, ale aj v kontexte článkov 24, 25 a 32 GDPR. Inými slovami, DPIA je špecifickým príkladom prístupu založeného na riziku pri spracovávaní údajov, v krátkosti ide o údaje, o ktorých sa predpokladá, že predstavujú vysoké riziko pre práva a slobody fyzických osôb, a žiada o rozsiahlejšie hodnotenie rizika a liečbu. V zásade však takéto hodnotenie rizika zahŕňa aj akúkoľvek ďalšiu kontrolu prípustnosti spracovania údajov vrátane adekvátnych technických a organizačných opatrení, ktoré minimalizujú riziko pred ich zavedením (pozri len článok 24 ods. 1 GDPR).

4.4. Proces DPIA

DPIA by sa malo vnímať ako proces (nielen ako správa), ktorý by sa mal začať čo najskôr ovplyvniť návrh predmetu ("projekt"). V dôsledku toho sa hodnotenie vplyvu líši aj od auditu, ktorý vyhodnocuje projekt ex-post a zvyčajne príde neskoro na to, aby "vyrovnal" potreby ochrany údajov, ktoré by DPIA mala produkovať.

Teraz existuje množstvo návrhov na implementáciu procesu DPIA, ktorý sa podobným spôsobom podobá výsledkom štúdie PIAF (2012), v ktorej sa zmapovali metodiky hodnotenia vplyvu na súkromie v siedmich krajinách (vrátane derivácie "najlepšej praxe" odporúčania a hlavné prvky procesu hodnotenia vplyvu na súkromie) okrem iného pre Komisiu EÚ. Boli identifikované nasledujúce základné prvky:

1. Určenie, či je potrebné PIA (prahová analýza).
2. Identifikácia tímu PIA a stanovenie referenčného rámca.
3. Opis navrhovaného projektu [a identifikácia zainteresovaných strán].
4. Analýza informačných tokov a iných dopadov na súkromie.
5. Konzultácie so zainteresovanými stranami.
6. Riadenie rizík [Identifikácia rizík a možných riešení].
7. Kontrola dodržiavania právnych predpisov.
8. Formulovanie odporúčaní.
9. Príprava a zverejnenie správy [napr. Na webovej stránke organizácie].
10. Realizácia odporúčaní.
11. Externá kontrola a / alebo audit tretej strany.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

12. Prehodnotenie PIA, ak sa príslušný projekt zmení [Aktualizácia PIA v prípade zmien v projekte].

Model DPIA pre inteligentné siete a inteligentné meracie systémy, ktorý je výslovne uvedený v odporúčaní Európskej komisie 2014/724 / EÚ, stanovuje tieto kroky:[3]

1. Krok 1 Predbežné hodnotenie a kritériá určujúce potrebu vykonať DPIA.

2. Krok 2 Začatie.

3. Krok 3 Identifikácia, charakterizácia a opis inteligentných sieťových systémov / aplikácií spracúvajúcich osobné údaje.

4. Krok 4 Identifikácia príslušných rizík.

5. Krok 5 Posúdenie rizika ochrany údajov.

6. Krok 6 Identifikácia a odporúčanie kontrol a zvyškových rizík.

7. Krok 7 Dokumentácia a vypracovanie správy DPIA.

8. Krok 8 Preskúmanie a údržba

Nová norma ISO / IEC 29134 poskytuje usmernenia pre proces vykonávania posúdení vplyvu na súkromie a pre štruktúru a obsah správy PIA. Proces je rozdelený na nasledovné štyri čiastkové procesy:

1. Prahová analýza.

2. Príprava PIA.

3. Vykonajte PIA.

4. Kontrola PIA.

V ktorom bode a v koľkých častiach je proces DPIA rozdelený, je to vec výberu, ďalšie návrhy sa pohybujú napríklad v troch alebo štyroch fázach v šiestich až siedmich fázach. Skôr sa za dôležité považuje zrozumiteľná štruktúra a priebeh procesu, ktorý

3 Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, ABl L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

zohľadňuje najmä požiadavky čl. 35 (7) GDPR a odporúčania pracovnej skupiny zriadenej podľa článku 29.

4.5. Začlenenie dotktnutých osôb alebo ich zástupcov

Podľa článku 35 ods. 9 správca údajov, ak je to vhodné, skúma názory dotknutých osôb alebo ich zástupcov na zamýšľané spracovanie bez toho, aby bola dotknutá ochrana obchodného alebo verejného záujmu alebo bezpečnosť spracovateľských operácií. Zahrnutie slova "podľa potreby" v súvislosti s rokovaniami o trialógu spôsobuje, že nie je jasné, za akých okolností by sa konkrétne malo získať postavenie dotknutej osoby alebo jej zástupcu a v akých prípadoch (prípustné) to možno upustiť.

Spôsob, akým sa požaduje stanovisko, je citlivá na kontext a WP29 uznáva rôzne spôsoby, ako je vykonanie štúdie (internej alebo externej), formálne rozhovory so zástupcami zamestnancov alebo odborových zväzov a predloženie dotazníka budúcim zákazníkom radič. Zo samotného znenia je možné vyvodiť len stanovisko (v pôvodnej verzii stanovísk komisie), nie však povinnosť brať do úvahy alebo dokonca požiadavku (nového) súhlasu (nad rámec zákona o ústavnej zmluve (ArbVG)) zamestnaneckej rady ako zástupca dotknutých osôb. Napriek tomu sa kontrolór bude musieť zaoberať stanoviskami dotknutých osôb alebo ich zástupcami a bude sa ich musieť zaoberať v hodnotení vplyvu. Či združenia na ochranu spotrebiteľa môžu byť zahrnuté pod pojem "zástupca", je kontroverzná v literatúre[4].

V každom prípade sa povinnosť konzultovať ***výslovne*** bez toho, aby bola dotknutá ochrana obchodných alebo verejných záujmov alebo bezpečnosť operácií spracovania. Preto prevádzkovateľ môže v extrémne obmedziť alebo odmietnuť povinnosť poskytnúť dotknutým osobám alebo zástupcom informácie o zamýšľanom spracovaní podľa článku 35 ods. 9 (čo v tomto prípade povedie k tomu, že a priori zapojenie do článok 35 ods. 9 nie je možný, keďže existencia dostatočných informácií je sine qua non pre stanovisko príslušných osôb alebo ich zástupcov).

Pri vykonávaní hodnotenia vplyvu ochrany údajov sa v správe odporúča zdokumentovať dôvody, prečo nebolo získané žiadne alebo len obmedzené obsahové stanovisko, alebo získané stanovisko nebolo alebo len čiastočne bolo zohľadnené.

4 *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.6. Správa o vykonávaní hodnotenia vplyvu na súkromie

Treba poznamenať, že správa DPIA nie je skutočným cieľom DPIA, ale "prostriedkom na ukončenie" dokumentácie procesu (interného a externého). Správa by sa nemala podceňovať - dokumentuje implementáciu a výsledky a z dôvodov súladu sa treba vyhnúť pouhým "správam PRDPIA". Správa môže tiež slúžiť ako sprievodca a kontrolný zoznam pri vykonávaní DPIA.

Art. 35 GDPR obsahuje, trochu prekvapujúco, žiadnu výslovnú požiadavku na prípravu správy o vykonávaní DPIA. Skutočnosť, že pre prevádzkovateľa existuje povinnosť dokumentácie, je nepochybne a implicitne vyplýva z článku 35 ods. 7 GDPR a tiež z článku 5 ods. 2 GDPR (zodpovednosť) v spojení s článkom 24 ods. 1 GDPR a článkom 36 ods. 3 písm. E) (ktorý vyžaduje, aby orgán dohľadu poskytol "posúdenie vplyvu ochrany údajov uvedené v článku 35"). Preskúmanie požadované v článku 35 ods. 11 na posúdenie, či sa spracovanie vykonáva v súlade s DPIA, a či vyžaduje, aby sa výsledky hodnotenia vplyvu zachovali. Okrem toho podávanie správ o realizovaných PIA je v súlade s celosvetovou osvedčenou praxou v tejto oblasti (pozri časť IV.1.

Proces DPIA sa dopĺňa s dokumentáciou v zmysle "živého dokumentu", pričom sa začína dokumentáciou analýzy prahovej hodnoty v prípade, že nie je potrebné vykonať DPIA. Aj keď táto analýza dokazuje, že DPIA nie je potrebná a proces je prerušený, zodpovedný za jej zodpovednosť a dôkazy bude zodpovedný kontrolór. Táto písomná dokumentácia môže byť predložená dozornému orgánu v každom budúcom procese a bude sledovať interné úvahy a hodnotenia.

Pokiaľ ide o obsah, správa DPIA v podstate stanovuje postup (vrátane prezentácie faktov v zmysle systematického popisu celého predmetu testu - "cieľ hodnotenia") a výsledkov procesu DPIA. Tak ako v prípade samotného procesu DPIA, GDPR nestanovuje žiadne osobitné pravidlá pre vypracovanie správy DPIA. Avšak ako minimálny obsah sú vopred stanovené kritériá uvedené v pracovnej skupine na ochranu údajov podľa článku 29 v prílohe 2 k WP 248, ktoré sú v podstate založené na článku 35 ods. 7. ISO / IEC 29134 odporúča nasledujúci obsah správy o hodnotení vplyvu na súkromie s dôrazom na hodnotenie rizika:

1. Príslušné požiadavky na ochranu súkromia.
2. Opis rozsahu.
3. Opis použitých kritérií rizika.
4. Účastníci implementácie.
5. Konzultované zainteresované strany.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Toto sa potvrdzuje aj odôvodnením č.90, v ktorom sa o.i.uvádza:" Toto posúdenie vplyvu by malo zahŕňať predovšetkým opatrenia, záruky a mechanizmy plánované na zmiernenie tohto rizika, zabezpečnie ochrany osobných údajov a preukázať súlad s týmto nariadením."

V podrobnej štúdii PIAF je minimálny obsah správy PIA náaseldovný: [5]

1. Úvod a základné informácie vrátane toho, kto vykonal PIA, jej kontaktné údaje a kde nájsť ďalšie informácie a ďalšie zdroje pomoci a poradenstva
2. Opis projektu, informačných tokov a vplyvov na súkromie.
3. Výsledky konzultácií so zainteresovanými stranami
4. Opis fázy posúdenia rizika a zmierňovania rizika vrátane zvažovaných alternatív.
5. Analýza dodržiavania právnych predpisov.
6. Odporúčania.
7. Prílohy, ak je to potrebné.

V prípade, že je k dispozícii správa alebo konečný návrh, môže nastať otázka, čo sa má robiť so zodpovednou (vnútornou) osobou, a to predovšetkým či a kým ju má schváliť - prakticky relevantný bod, ktorý zostane nezmenený GDPR. ICO vo svojom Kódexe pravidiel výslovne stanovuje nasledovné: "[o] udržiať vhodné podpisy v rámci organizácie". Keďže zodpovedná osoba musí vykonať DPIA, z toho vyplýva, že do DPIA sú zapojení príslušne poverení zástupcovia zodpovednej osoby a majú aj konečnú zodpovednosť. Úroveň riadenia bude mať zvyčajne konečnú rozhodovaciu právomoc nad predmetom a povahou projektu DPIA. Ako minimálny variant by mal manažér projektu alebo úradník pre ochranu údajov podávať správy na "najvyššej riadiacej úrovni", ako je ustanovené v čl. 38 (3) GDPR.

GDPR nie je povinná uverejňovať DPIA, ale WP29 odporúča jeho publikovanie (aspoň čiastočne) s cieľom zvýšiť dôveru v spracovanie údajov a podporiť transparentnosť. Publikácia sa odporúča najmä v prípadoch, keď časť ("plánované") spracovanie ovplyvní časť verejnosti.

5. Záver a praktické typy

Predovšetkým regulačné agentúry s kvalitnými zdrojmi vyvinuli vlastné prístupy pre hodnotenie vplyvu na súkromie v priebehu niekoľkých rokov. Z dnešnej perspektívy

5 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

možno očakávať, že orgány pre ochranu údajov, ktoré už vyvinuli svoj vlastný model, budú uprednostňovať alebo šíriť to, hlavne preto, že znalosti príslušného dozorného orgánu o ich vlastných odporúčaniach budú najvýraznejšie. Obsah aktuálne dostupných modelov vnútroštátnych orgánov dohľadu (z členských štátov EÚ) je často pred GDPR a nie je (zatiaľ) dôsledne prispôsobený požiadavkám alebo terminológii GDPR.

Medzinárodná organizácia pre medzinárodnú spoluprácu (ICO) však pridala do svojho štandardu PIA (2014) správu "Veľké údaje, umelej inteligencie, strojové učenie a ochrana údajov" (požiadavky na čítanie) a terminológiu GDPR, orgánov. Je potrebné zistiť, či Európska rada pre ochranu údajov (článok 68) poskytne usmernenia, odporúčania a / alebo osvedčené postupy pre DPIA v súlade s čl. 70 ods. 1 písm. E).

Odporúčania na prvý pohľad:

- Dokumentácia všetkých rozhodnutí, najmä dôvod, pre ktorý nebol vykonaný DPIA (ak je to vhodné);
- Ak máte pochybnosti, vykonajte DPIA:
- Zapojenie interných a externých zainteresovaných strán;
- Používanie modelov, osvedčených postupov a, ak je to vhodné podobných DPIA už existujúcich
- Publikovanie DPIA:
  - najmä verejnými orgánmi;
  - zvyšuje informovanosť o ochrane súkromia a zvyšuje dôveru.

6. Externé zdroje a webové linky

6.1. Bibliografia a literatúra

- ***Kastelitz, M., Hötzendorfer, W., Riedl, R***., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.
- ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- ***Wright, David/De Hert, Paul*** **(Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012
- ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

6.2. Dokumenty článku 29 Working Party – pracovná časť/strana

- Artikel-29-Working Party, WP 248, April 4, 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- WP 248, as last Revised and adopted on 4 October 2017 (rev.01): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Impact_Assessment_(DPIA).pdf/ed5daa8c-d388-43a6-9842-629b8175a99c

6.3. Webové Linky

- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/
- ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).