SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

Průzkum SPDČR k implementaci obecného nařízení o ochraně osobních údajů (GDPR) mezi členskými firmami

ÚVOD

Dotazník měl upozornit firmy na nový právní akt EU, na jehož účinnost by se měly dobře připravit, ačkoli nastane „až" v květnu roku 2018 – tj. na Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů" nebo „GDPR").

ČR z důvodu adaptace na nařízení přijme velkou novelu zákona na ochranu osobních údajů, případně připraví zákon zcela nový. Měnit se bude i celá řada souvisejících zákonů jako například zákoník práce či zdravotnická legislativa. **Aplikace nových povinností stanovených nařízením bude zcela jistě znamenat finanční, organizační a personální náklady pro podniky, které jsou správci nebo zpracovateli osobních údajů.**

Cílem tohoto dotazníku bylo jednak zjistit obecné povědomí a míru připravenosti firem na aplikaci tohoto nařízení, jednak identifkovat oblasti, které budou v rámci adaptace pro firmy nejvíce problematické. Tato zjištění budou dále rozpracována a využita při jednáních s vládou ČR a regulátorem s cílem eliminovat zbytné zvýšení finanční a administrativní zátěže i pro osvětu a podporu implementace mezi firmami.

Šetření probíhalo na září/říjen 2016. V úvodu dotazníku byl krátký výklad cíle nařízení a shrnutí jeho nejdůležitější oblasti, každá otázka pak byla doplněna vysvětlením. Osloveny byly členské firmy SP ČR, to znamená jak individuální členové (136 firem), tak 31 kolektivních členů (svazů a asociací). Návratnost 209 dotazníků považujeme za vysokou také vzhledem komplexnosti nařízení a z něho vyplývající složitosti dotazů.

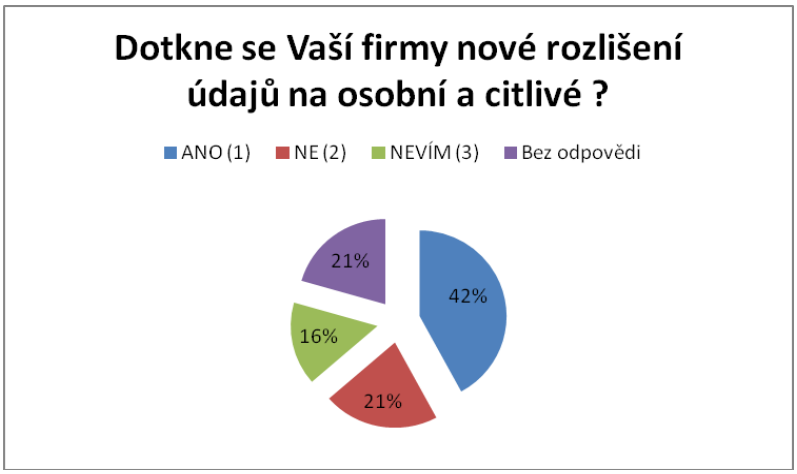
Za zajímavé a vypovídající považujeme i komentáře firem k jednotlivým položeným otázkám.

1. DEFINICE OSOBNÍCH ÚDAJŮ PODLE NAŘÍZENÍ GDPR (ČLÁNEK 4)

1a) Dotkne se Vaší firmy nové rozlišení údajů na osobní a citlivé?

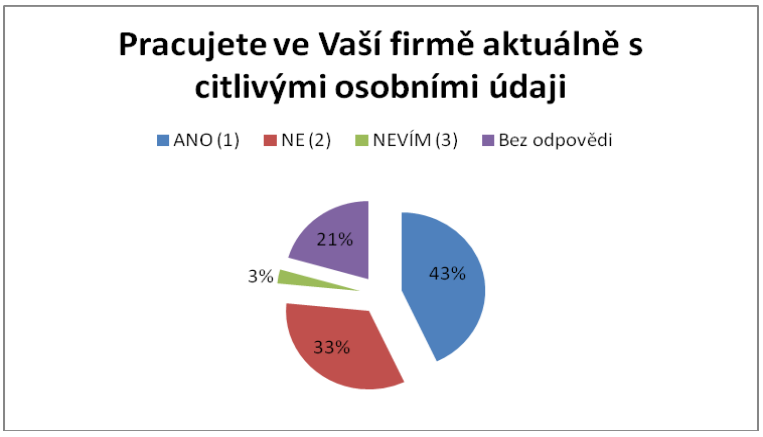
Odpověď	Počet	Procenta
ANO (1)	88	42.11%
NE (2)	45	21.53%
NEVÍM (3)	33	15.79%
Bez odpovědi	43	20.57%

TELEFON (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

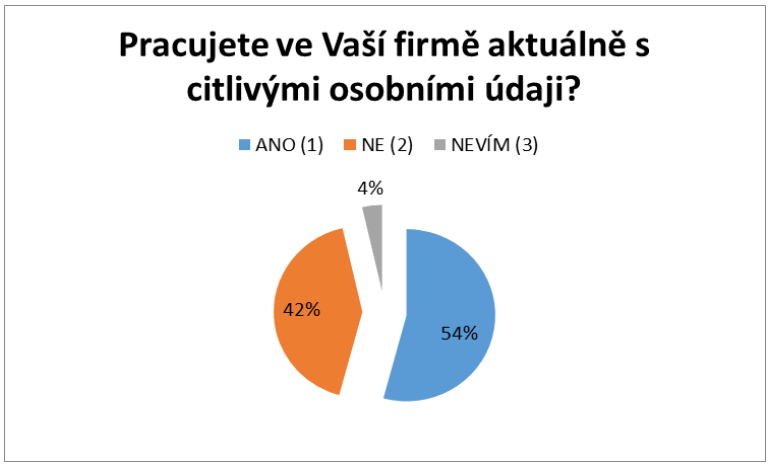


1b) Pracujete ve Vaší firmě aktuálně s citlivými osobními údaji?

Odpověď	Počet	Procenta
ANO (1)	90	43.06%
NE (2)	70	33.49%
NEVÍM (3)	6	2.87%
Bez odpovědi	43	20.57%



Pokud vycházíme pouze z těch firem, které na otázku odpověděly, je procentuální rozložení následující:



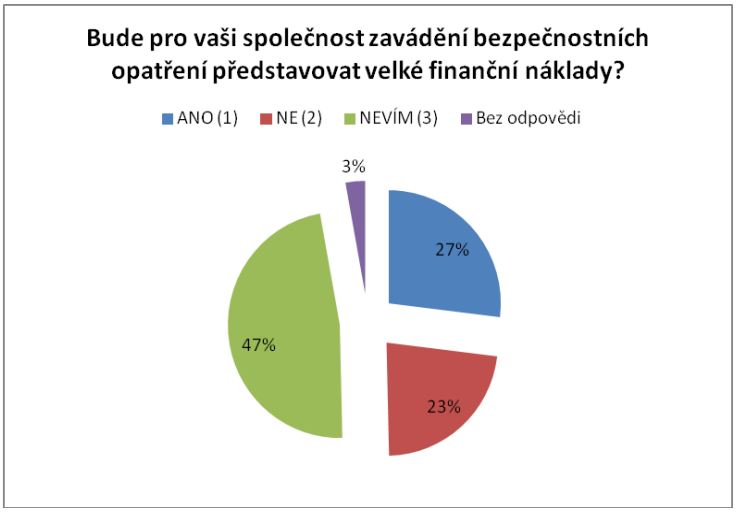
Komentáře firem:

- Citlivým údajem i nadále zůstává "členství v odborových organizacích".
- Každý zaměstnavatel řeší zdravotní stav zaměstnanců, a proto disponuje i citlivými údaji.
- Naše společnost pracuje s osobními citlivými údaji pouze ve formě potvrzení o vstupní a preventivní zdravotní prohlídce, jak předepisuje zákon.
- Pokud jsou preventivní nebo periodické profesní prohlídky osobním citlivým údajem, potom platí ANO.
- Uvedu příklad konfliktní situace: ve firmě existují práce zakázané těhotným ženám, ale firma se ženy na těhotenství nesmí ani zeptat, natož jej nějak evidovat.
- V našem konkrétním případě bude osobním citlivým údajem posouzení zdravotního stavu zaměstnance prováděné závodním lékařem při nástupu zaměstnance do pracovního poměru a s ohledem na kategorizaci pracovních míst i posuzování zdravotního stavu periodicky. S ostatními jmenovanými citlivými údaji nepracujeme.
- Veškeré firmy pracují osobními údaji, které mohou spadat do "citlivé", jedná se o údaje o zdravotním stavu, zda se jedná o zaměstnance se ZPS či jiným omezením, ale již konkrétní zdravotní stav není zkoumám, a proto by se mělo jednat pouze o osobní údaj.
- Výsledky lékařských prohlídek nutných pro výkon práce.
- Zde předpokládáme, že zdravotní údaj o schopnosti vykonávat příslušnou pracovní pozici nebude řazen k citlivým údajům.
- Ze zákona musí každý zaměstnavatel zajistit, aby zaměstnanci byli odborně a zdravotně způsobilí. Pokud je citlivým údajem údaj o zdravotním stavu, tak pouhá informace, že je zdráv a schopen práce, je citlivým údajem, který má každý zaměstnavatel k dispozici.

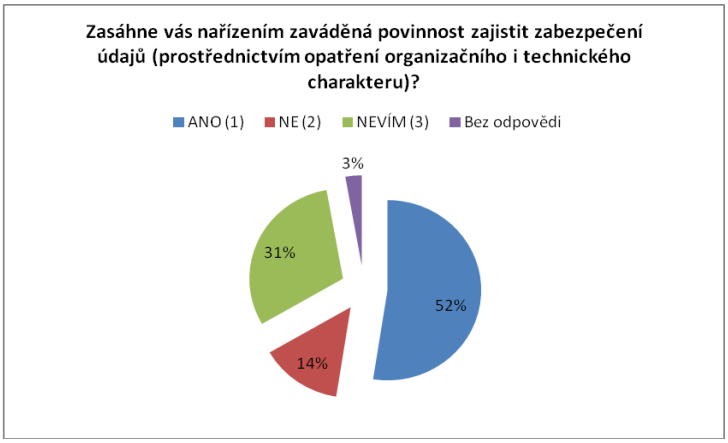
2. ZABEZPEČENÍ ZPRACOVÁNÍ (ČLÁNEK 32)

2a) Používáte při zpracování osobních údajů ve Vaší firmě opatření pro zabezpečení zpracování údajů?

2b) Bude pro vaši společnost zavádění bezpečnostních opatření představovat velké finanční náklady?

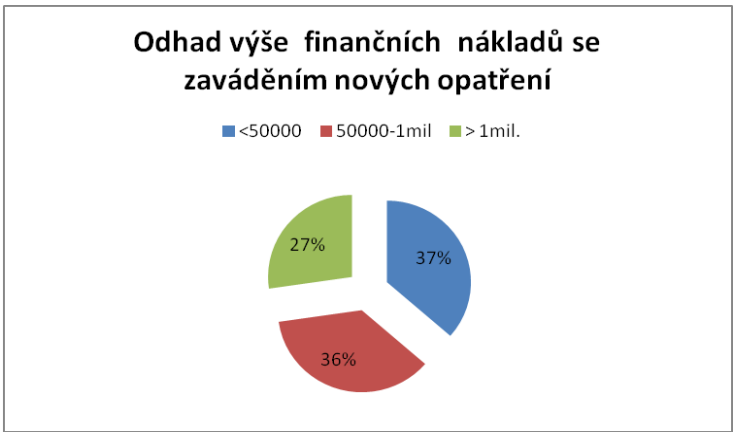


2c) Zasáhne vás nařízením zaváděná povinnost zajistit zabezpečení údajů (prostřednictvím opatření organizačního i technického charakteru)?



V případě, že se zaváděním nových opatření budete mít finanční náklady, pokuste se, prosím odhadnout jejich výši.

Na tuto otázku odpovědělo pouze 6% dotázaných.

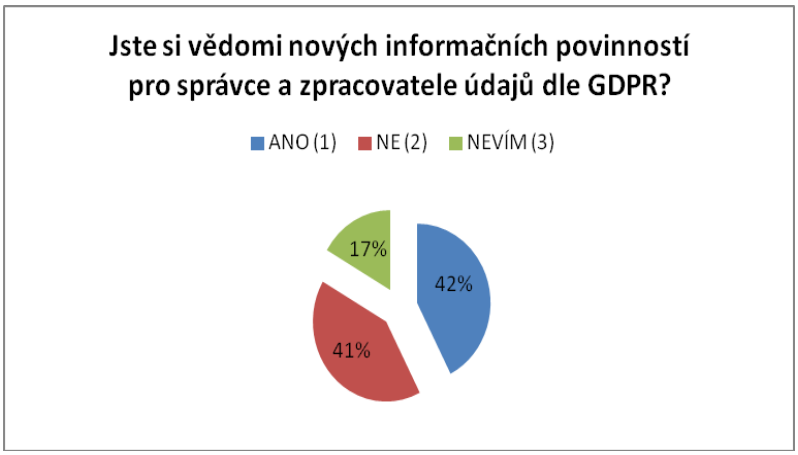


Komentáře firem:

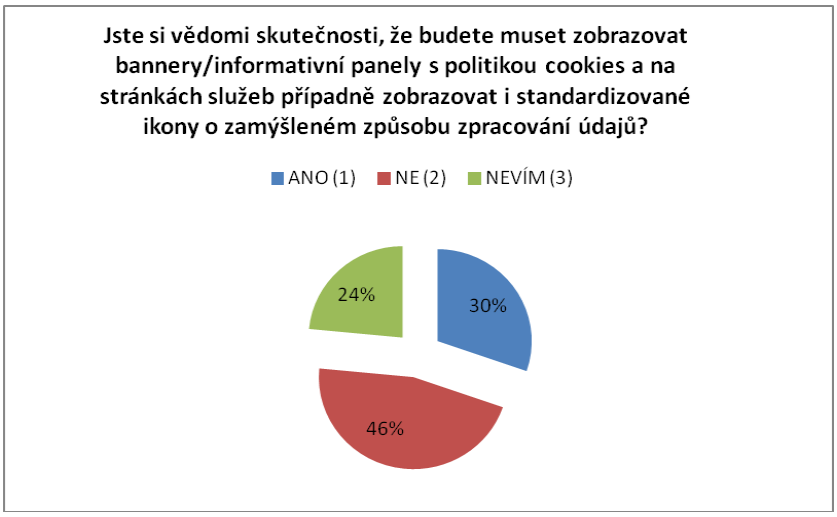
- Bezpečnost svých dat neumí zajistit ani Pentagon, to co nové předpisy požadují je úmyslné zhoršování konkurenceschopnosti firem. Každé náklady ovlivňují ceny produkce a dovedu si živě představit, jak podobné zabezpečení mají ve svých nákladech např. čínské, ale i jiné firmy.
- Finanční dopady pro společnost poskytující cloudové služby jsou v současné době nevyčíslitelné. Budou však značně vysoké.
- Myšlenka pseudonymizace osobních údajů na úrovni výrobních podniků je tak šílená, až je zábavná.
- Náklady zatím neumím odhadnout.
- Nařízení byrokratizuje proces ochrany osobních údajů. Mnoho úkonů, které požaduje, jsou de facto formální a tedy finančně a morálně drahé.
- Opatření k zabezpečení osobních údajů jsou z větší části již provedena, počkáme na legislativní úpravu. Nemůžeme proto definovat možné náklady.
- Otázkou zůstává, zdali může jít pouze o náklady naší společnosti anebo budou chtít nějakou kompenzaci nákladů i lékaři poskytující zdravotně lékařskou péči.
- Řádově desítky až stovky tisíc.
- Těžko dnes odhadnout náklady na úpravu sw.
- Vůbec nevím, co všechno bude nařízení obnášet, natož odhadnout náklady na zabezpečení.

3. INFORMAČNÍ POVINNOST

3a) Jste si vědomi nových informačních povinností pro správce a zpracovatele údajů dle GDPR?

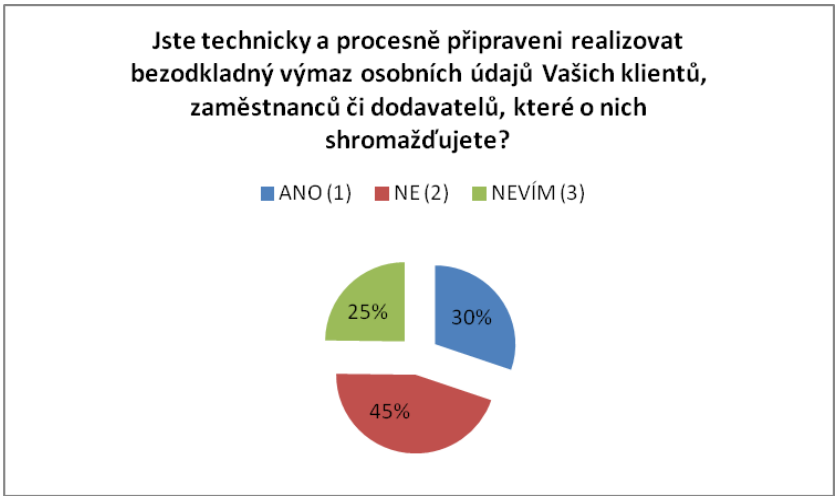


3b) Jste si vědomi skutečnosti, že budete muset zobrazovat bannery/informativní panely s politikou cookies a na stránkách služeb případně zobrazovat i standardizované ikony o zamýšleném způsobu zpracování údajů?



4. PRÁVO NA VÝMAZ OSOBNÍCH ÚDAJŮ („PRÁVO BÝT ZAPOMENUT“) (ČLÁNEK 17)

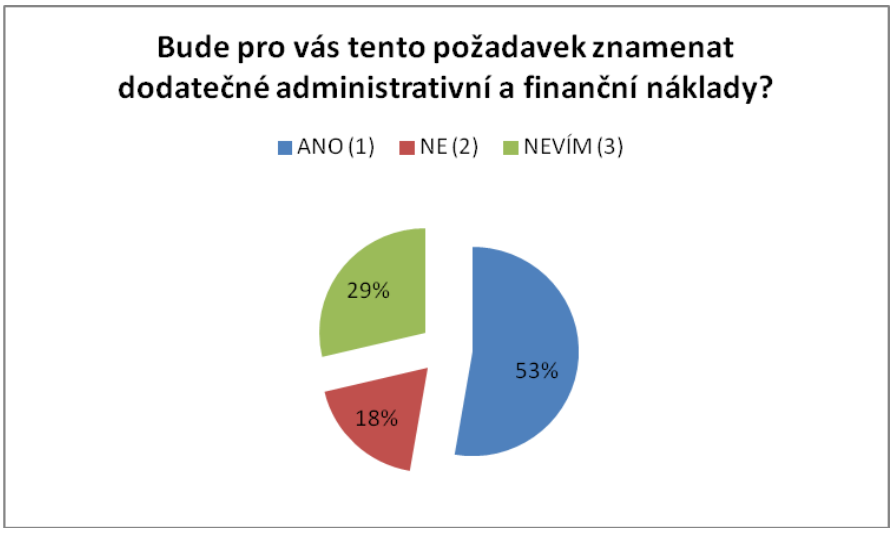
4a) Jste technicky a procesně připraveni realizovat právo subjektu údajů na bezodkladný výmaz osobních údajů, které o něm shromažďujete?



Komentáře firem

- Jelikož jsem si Nařízení EU pročetla, něco o tom vím, ale detail neznám.
- Nemyslíme, že se nás tyto povinnosti budou týkat.
- Uvědomují si vůbec tvůrci legislativy, že se bude dotýkat i malých a středních firem, ve kterých všechnu administrativní činnost vykonává jen několik lidí? Asi ano a chtějí je tímto způsobem postupně zlikvidovat.
- Zajímavé bude, co nám poslanci nadělí. To zatím nevíme.

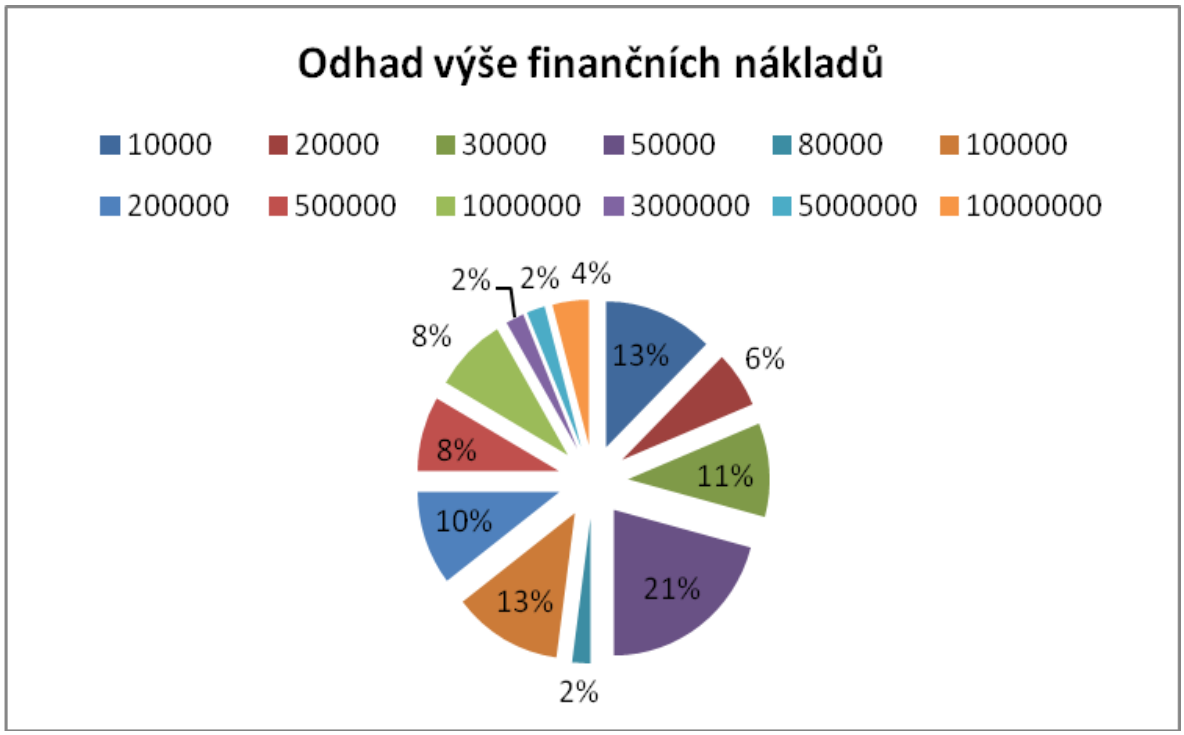
4b) Bude pro vás tento požadavek znamenat dodatečné administrativní a finanční náklady?



Komentáře firem:

- Asi ano ale vzhledem k tomu že neznám detaily nemohu se blíže vyjádřit
- Jelikož nevíme, zda budou dodatečné náklady, odpověděli jsme NE.
- Ono je to v řadě případů prakticky nerealizovatelné. Nevymažete ty údaje ze všech záloh. Něco vymazat nemůžete, máte povinnost z jiného zákona ta data držet. Jak se bude řešit tento střet-
- Spíše se jen domnívám, že ano.
- Technicky ano, procesně ne
- to je snad zbytečná otázka. Každá činnost navíc představuje nějaké náklady a ty vždy sníží konkurenceschopnost.
- Výmaz záznamů zaměstnanců by byl protizákonný. Osobní údaje klientů neshromažďujeme.
- vzhledem k tomu, že jsme zatím neřešili, netuším, co by případné zavedení znamenalo administrativně a finančně

V případě, že se zaváděním nových opatření budete mít finanční náklady, pokuste se, prosím odhadnout jejich výši.

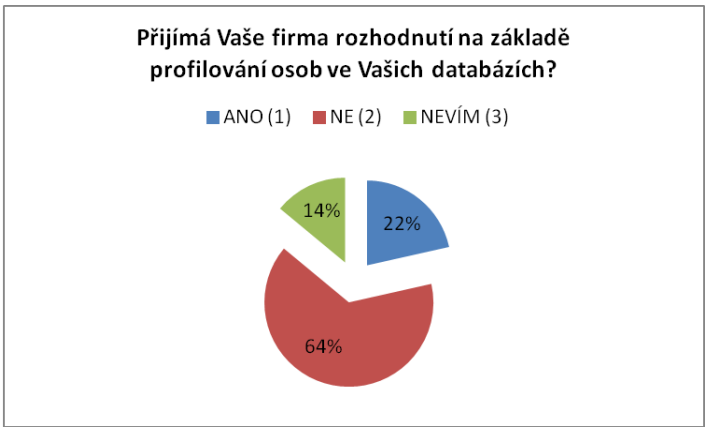


Komentáře firem:

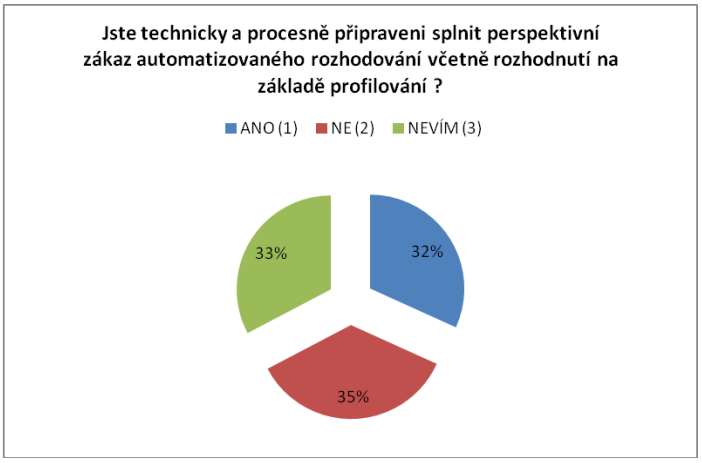
- Jsem zvědav, jak budeme plnit požadavek na výmaz údajů zaměstnanců, když jine zákony požadují jejich mnohaleté uchovávaní. (Mnohdy duplicitně se statni správou- viz evidenční listy, doklady o nemocenské atd...)
- Jsme střední firma, nemám k disposici aparát, který by se podobnými prognózami mohl zabývat
- Náklady netuším. Proč musím psát do té rubriky výše číslo, když to prostě nevím.
- Skutečně nedokážu odhadnout.
- Technická a procesní připravenost pro výmaz - u hlavních HR systémů ano u ostatních ne.
- V tento okamžik nejsme schopni přesného finančního odhadu, ale bude v řádu desítek miliónů
- Výmaz osobních údajů o zaměstnancích v pracovním poměru nelze provést, personální údaje o zaměstnancích po ukončení pracovního poměru podléhají skartačnímu řádu.

5. AUTOMATIZOVANÉ INDIVIDUÁLNÍ ROZHODOVÁNÍ VČETNĚ PROFILOVÁNÍ (ČLÁNEK 22)

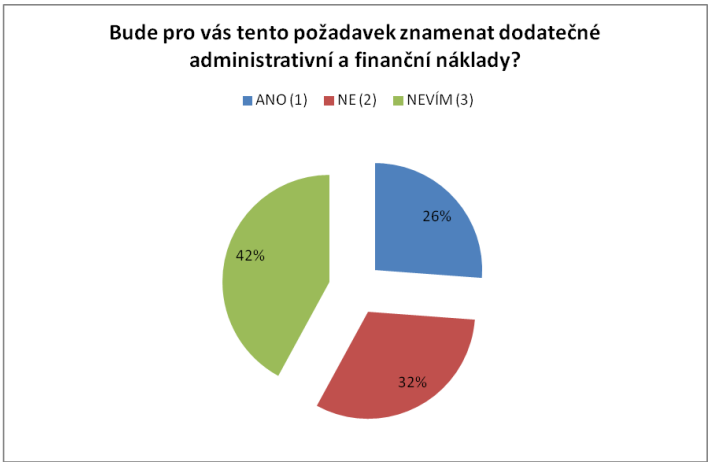
5a) Přijímá Vaše firma rozhodnutí na základě profilování osob ve Vašich databázích?



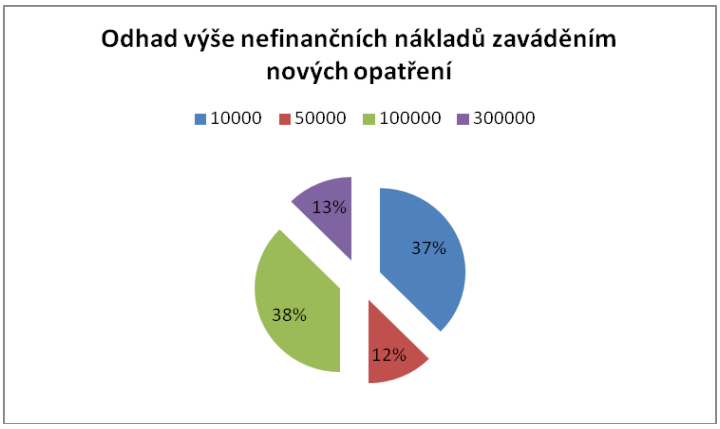
5b) Jste technicky a procesně připraveni splnit perspektivní zákaz automatizovaného rozhodování včetně rozhodnutí na základě profilování?



5c) Bude pro vás tento požadavek znamenat dodatečné administrativní a finanční náklady?



V případě, že se zaváděním nových opatření budete mít finanční náklady, pokuste se, prosím odhadnout jejich výši.

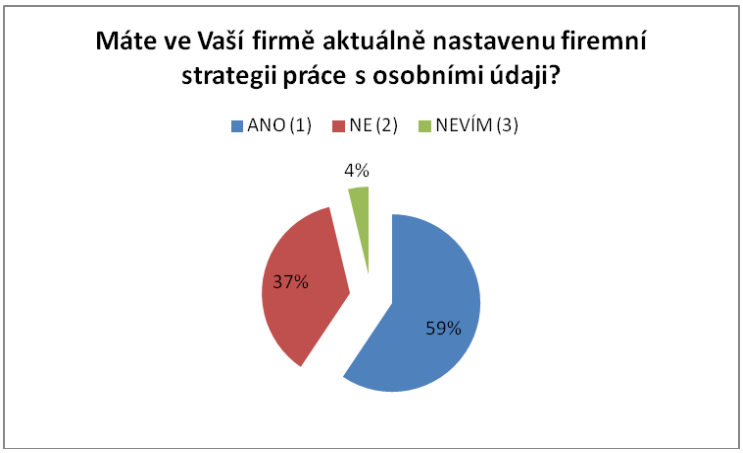


Komentáře firem:

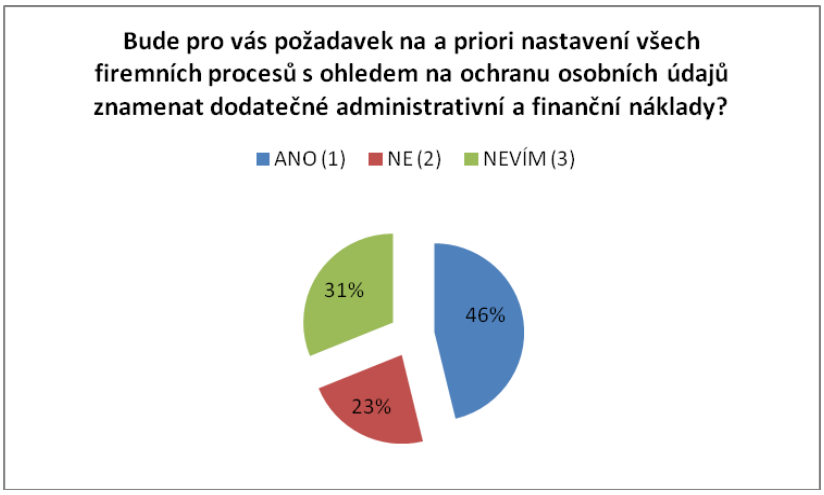
- Ani nevím, o čem ty otázky jsou. Jsme středně velká výrobní firma. Udělali si tvůrci těchto nařízení analýzy, jaké náklady na podobné činnosti vynakládají srovnatelné firmy ve světě mimo EU (a možná USA)? Nejspíš žádné, protože nevěřím, že by se takovými otázkami vůbec zabývali.
- K rozhodnutí NE, k marketingovým aktivitám ANO.
- Nedokážu odhadnout.
- Nepředpokládáme, že bychom někdy takové automatizované zpracování zaváděli.

6. STANDARDY OCHRANY OSOBNÍCH ÚDAJŮ (ČLÁNEK 25)

6a) Máte ve Vaší firmě aktuálně nastavenu firemní strategii práce s osobními údaji?



6b) Bude pro vás požadavek na a priori nastavení všech firemních procesů s ohledem na ochranu osobních údajů znamenat dodatečné administrativní a finanční náklady?

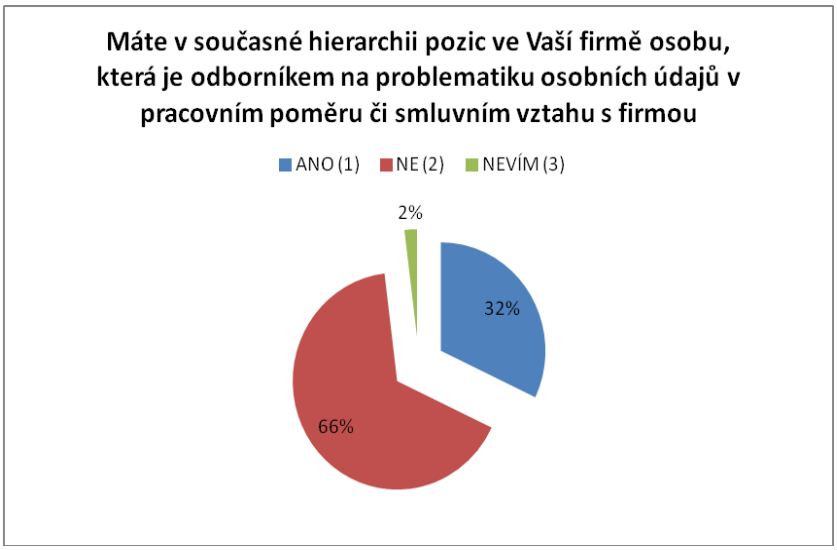


Komentáře firem:

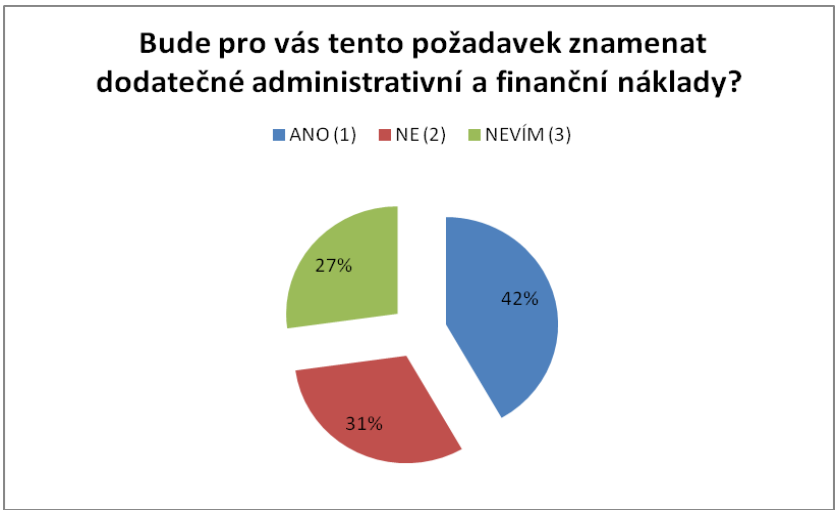
- Aktuálně probíhá tzv. readiness assessment a hodnocení dopadů do procesní a datové architektury společnosti.
- Co je cílem tvůrců (a schvalovatelů) těchto předpisů? Zlikvidovat malé a střední podniky!
- Údaje o našich klientech jsou již teď důvěrné. Povaha našich služeb se nezmění.
- Určitě bude zapotřebí právní, tedy ne zrovna levná, analýza současného stavu a požadavků na změnu v práci s osobními údaji. V personální práci pak může nastat významnější problém v oblasti práce s uchazeči o zaměstnání.
- Zpracováním dokumentu, který popíše naši dosavadní praxi, a zda tomuto nařízení vyhovíme. Na viržinkách už, zdá se, nebude moci být údaj balil.

7. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ (DATA PROTECTION OFFICER) (ČLÁNEK 37)

7a) Máte v současné hierarchii pozic ve Vaší firmě osobu, která je odborníkem na problematiku osobních údajů v pracovním poměru či smluvním vztahu s firmou, podílí se na rozhodování firmy a současně není přímo zapojena do práce s osobními údaji?



7b) Bude pro vás tento požadavek znamenat dodatečné administrativní a finanční náklady?



7c) Plánujete vytvořit pozici interně nebo ji zajistit jako externí službu?

Plánujete vytvořit pozici interně nebo ji zajistit jako externí službu?

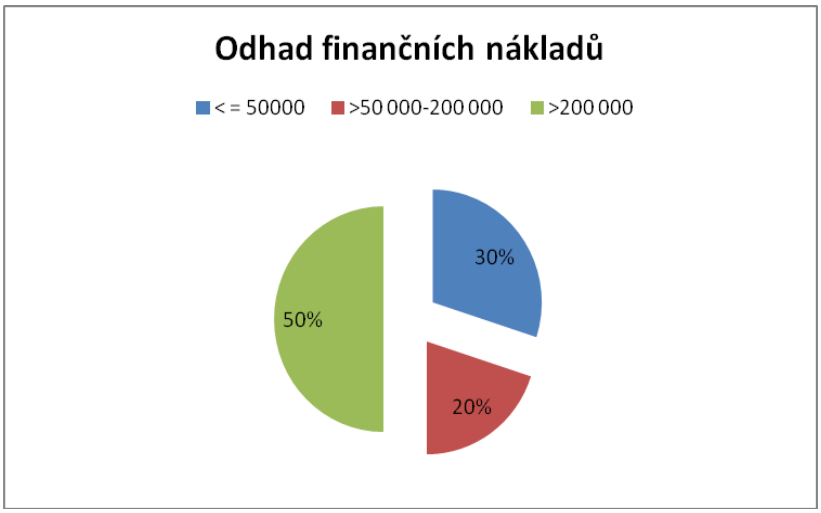
Odpověď	31	14.83%
Bez odpovědi	72	34.45%
Nekompletní	106	50.72%

Forma	četnost odpovědí
Externě	3
Interně	10
Ne	8
Nevím	5

Komentáře firem:

- Nevytvoříme tuto pozici vůbec!
- Pořizujeme softwarovou podporu s možností úplné kontroly nad jejich distribucí.
- Mají tvůrci těchto předpisů představu, jak to řešit v malých a středních firmách - samozřejmě jedině externím pracovníkem, nebo firmou. Takže to je další nádherný, a zcela neproduktivní job pro tisíce "nových odborníků" po celé Evropě.
- Měli jsme odpovědnou osobu, nyní máme pouze osobu, která to okrajově zastřešuje, tudíž bude muset upravit pracovní náplň.

7d) V případě, že se zaváděním nových opatření budete mít finanční náklady, pokuste se, prosím odhadnout jejich výši.

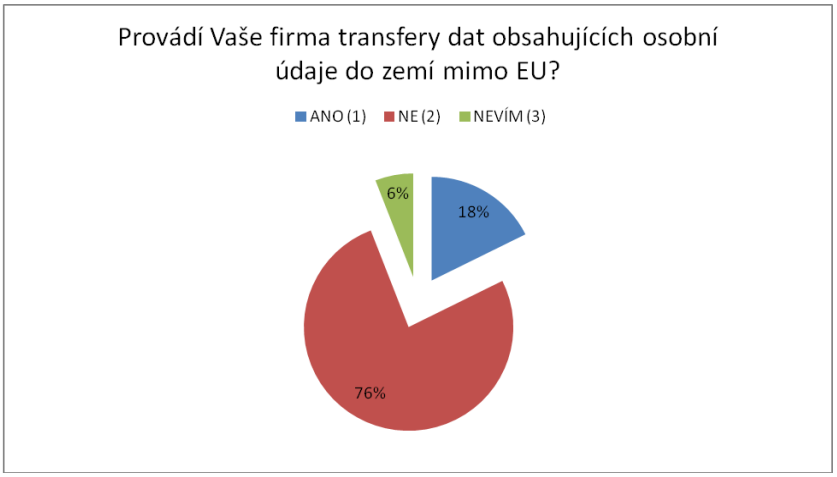


Komentáře firem:

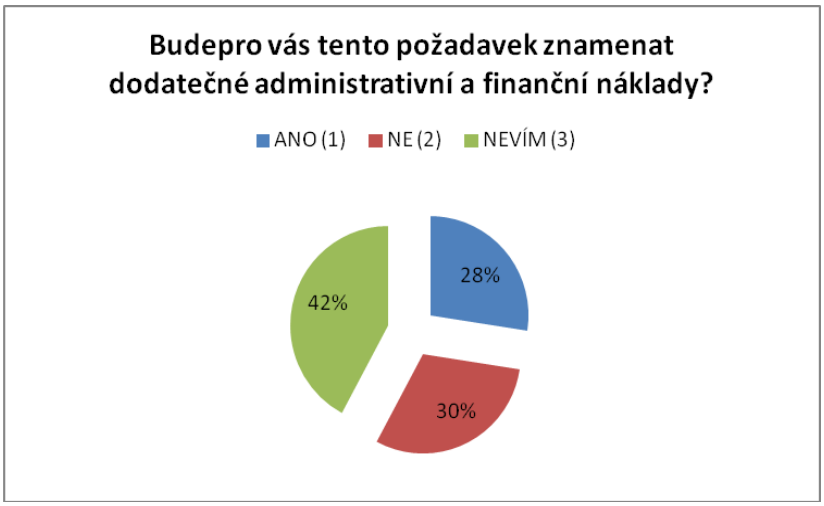
- (50% kapacity je určena na ochranu personálních dat)
- Nedokážu posoudit rozsah činností s nově vzniklou pozicí spojených, zda půjde řešit kumulací pozic a pod.
- Nemáme zatím vyjasněno.
- Tato povinnost se nebude vztahovat na subjekty, které vedou běžnou personální agendu zaměstnanců.
- Tento požadavek je nesmyslný a proto neproveditelný. Osoba s touto předpokládanou kvalifikaci, která zároveň s údaji nepracuje, je fikce. Každá činnost vyžaduje jiné údaje ať osobni nebo citlivé a citovaná osoba by musela všemu rozumět - např. požadavky BOZP, PO, na mzdovou agendu atd.

8. MEZINÁRODNÍ DATOVÉ TRANSFERY A PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ MEZINÁRODNÍM ORGANIZACÍM (ČLÁNEK 44 A NÁSLEDUJÍCÍ)

8a) Provádí Vaše firma transfery dat obsahujících osobní údaje do zemí mimo EU?



8b) Jste technicky a procesně připraveni splnit požadavek na dokumentaci takových datových transferů a současně zajistit subjektům údajů stejnou míru ochrany, kterou garantuje GDPR?

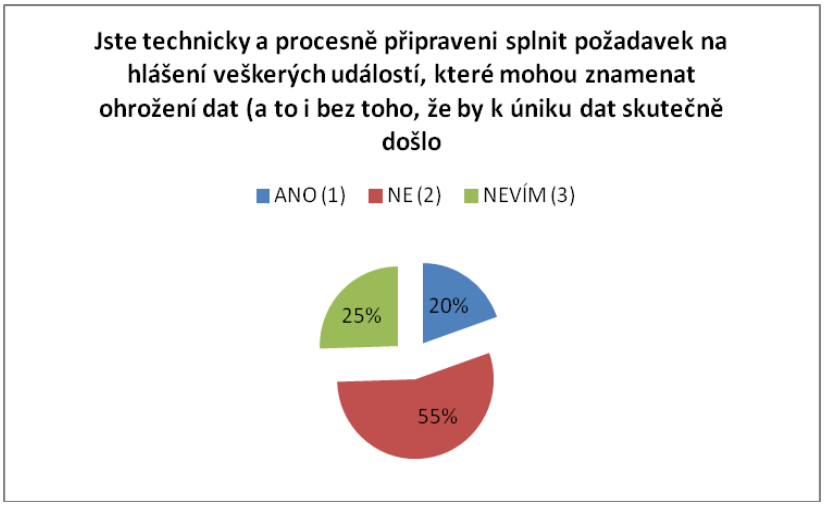


Komentáře firem:

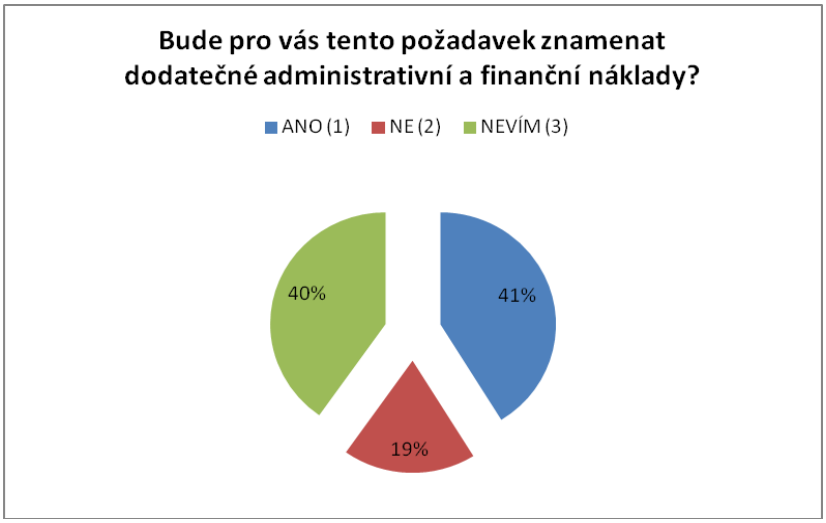
- Jsme součásti Privacy Shield USA, garantujeme bezpečný přenos dat do USA.
- Každá změna na pozici pracovníka, který s danými údaji přichází do styku už představuje riziko porušení zabezpečení. Tvůrci předpisů žijí ve virtuálním světě a zřejmě ani netuší, co se chystají spáchat.
- Nemyslíme si, že se nás toto nařízení týká.
- Probíhá certifikace dle Privacy Shieldu.

9. OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ DOZOROVÉMU ÚŘADU A SUBJEKTU ÚDAJŮ (ČLÁNEK 33 A NÁSLEDUJÍCÍ)

9a) Jste technicky a procesně připraveni splnit požadavek na hlášení veškerých událostí, které mohou znamenat ohrožení dat (a to i bez toho, že by k úniku dat skutečně došlo), do 72 hodin od jejich vzniku?



9b) Bude pro vás tento požadavek znamenat dodatečné administrativní a finanční náklady?



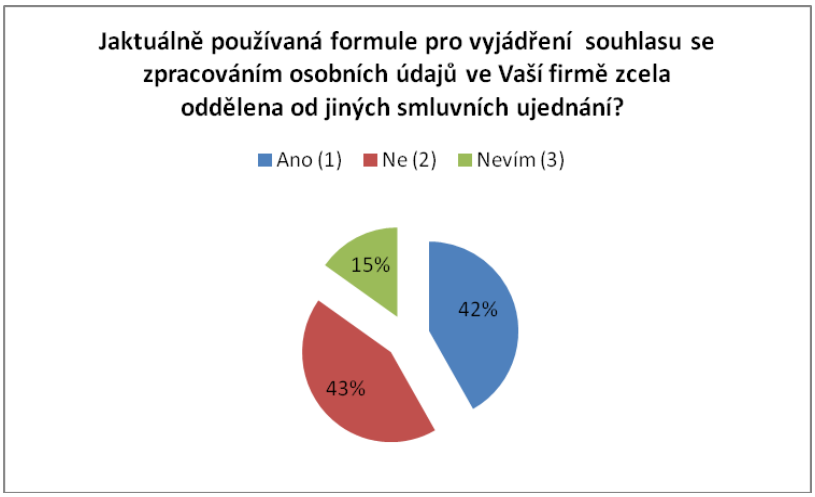
Komentáře firem:

- Na úrovni bezpečnosti je společnost připravena, ale v rámci datového managementu, který je s tématem úzce propojen si soulad s implementací GDPR vyžádá dodatečná opatření.
- Nemyslíme si, že se nás toto nařízení týká.
- Opět jeden z požadavků, který je nesmyslný a v důsledku nerealizovatelný u běžné společnosti, která nemá práci s daty jako svůj předmět podnikání. To nehovořím o zásadě, že žádný subjekt nesmí byt nucen svědčit proti sobe a problematičnosti samotného terminu "události, které mohou znamenat unik dat, i presto, že k němu nedošlo".

- Technicky a technologicky nejsme schopni kontrolovat únik elektronických dat a ani nám to legislativa v plném rozsahu neumožňuje.
- Už se mi nechce toto blouznění komentovat.

10. SOUHLAS S UDĚLENÍM SOUHLASU K POSKYTNUTÍ A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ (ČLÁNEK 7)

10a) Je aktuálně používaná formule pro vyjádření souhlasu se zpracováním osobních údajů ve Vaší firmě zcela oddělena od jiných smluvních ujednání?



Komentáře firem:

- Není zcela oddělena, tvoří však samostatnou kapitolu v rámci daného formuláře, vzhledem k všeobecným znalostem osobních práv občanů se to jeví jako postačující řešení.
- Někde je oddělena, někde není. Třeba v zaměstnaneckých smlouvách není.
- Součást Pracovní smlouvy.
- Souhlas se zpracováním osobních údajů od zaměstnanců nemáme, protože ho nepotřebujeme.

10b) Pokud ne, jaké kroky budete muset k zavedení této změny podniknout?

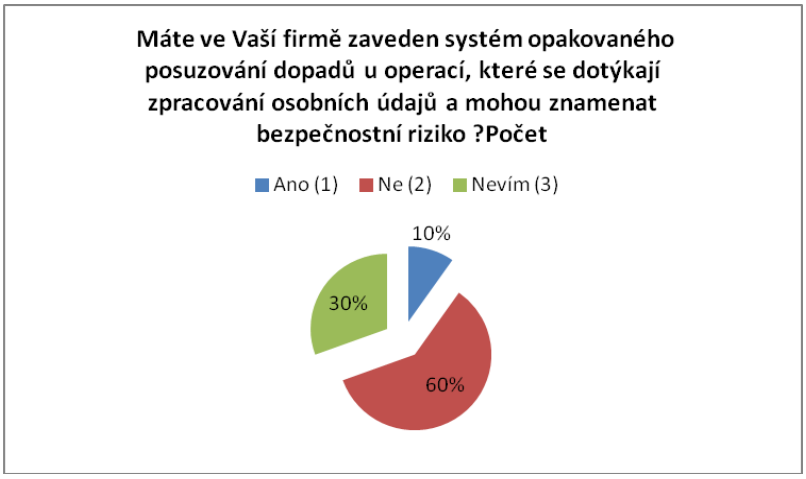
Komentáře firem:

- Bude specifikováno.
- Inu, jestliže nějaké zákonné nařízení nám tuto povinnost stanoví, dáme zaměstnancům tento souhlas podepsat. Kdo nepodepíše, bude propuštěn, protože nám neumožní plnit jiné zákonné povinnosti.
- Nový formulář.
- Oddělit to.
- Přepsat zaměstnanecké smlouvy.
- Připravit samostatný dokument Souhlas ke zpracování osobních údajů.
- Upravit znění některých smluvních ujednání.
- Vyčlenit souhlasy z pracovních smluv.
- Vydat v rámci zjednodušení agendy další formulář.
- Vytvoříme nový tiskopis.
- Vytvořit speciální dohody.

- Vyžádat odbornou konzultaci znalce, upravit formuláře, upravit aplikační software zaplatit provedení úpravy SW.
- Zavést další (jistě velmi užitečný a přispívající k tvorbě hodnot)papír pro všechny zaměstnance).

11. OPAKOVANÉ POSUZOVÁNÍ DOPADU (ČLÁNEK 35)

11a) Máte ve Vaší firmě zaveden systém opakovaného posuzování dopadů u operací, které se dotýkají zpracování osobních údajů a mohou znamenat bezpečnostní riziko?

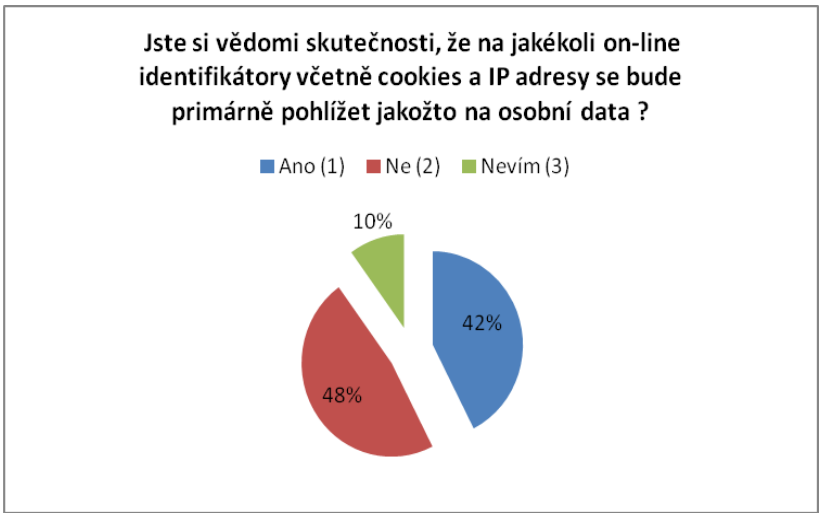


Komentáře firem:

- Asi budu uvažovat o ukončení podnikání
- Směrem k zákazníkům ano, interně bude potřeba provést další analýzu

12. ON-LINE IDENTIFIKÁTORY

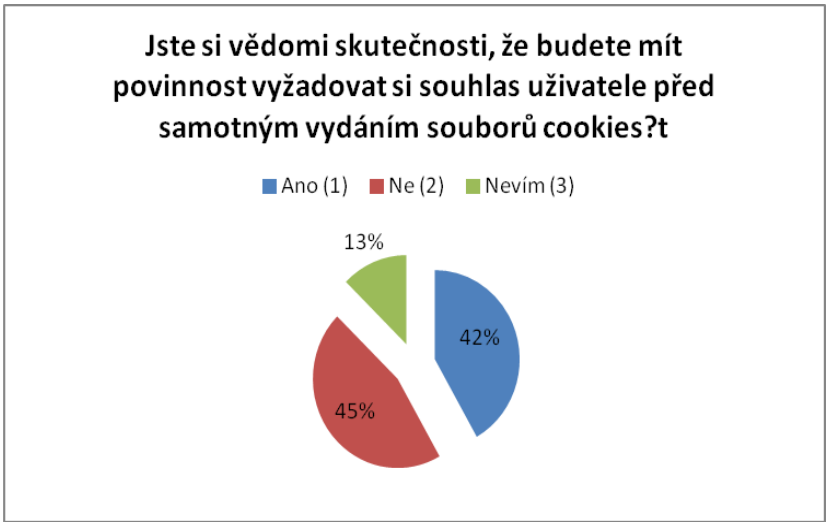
12a) Jste si vědomi skutečnosti, že na jakékoli on-line identifikátory včetně cookies a IP adresy se bude primárně pohlížet jakožto na osobní data?



Komentáře firem:

- Jak toto v dnešním přetechnizovaném a přeelektronizovaném světě může zabezpečit malá nebo střední firma- znovu opakuji: data unikají i Pentagonu a nyní chcete v Evropě zavést tyto povinnosti- vždyť běžný člověk ani nemá tušení, kde všude mohou tyto údaje po sítích kolovat.
- Jsem si vědoma jen díky tomu, že jsem si načetla v novém Nařízení EU.
- Netýká se nás.

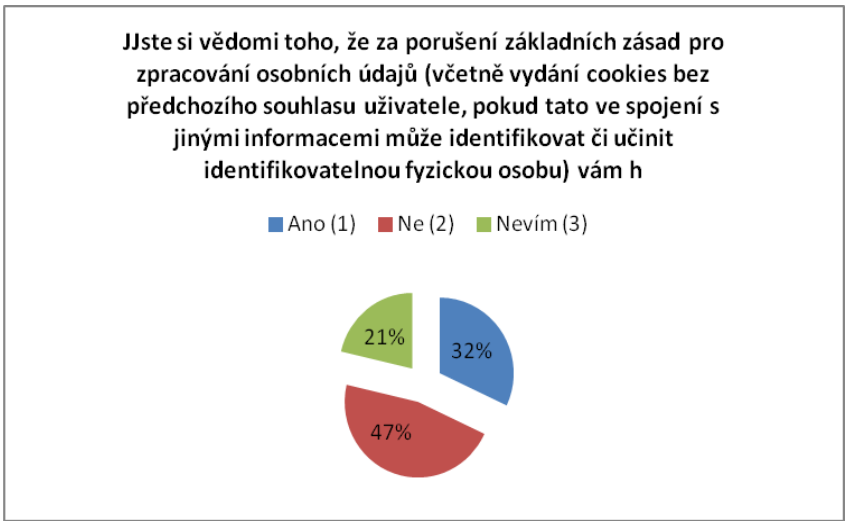
12b) Jste si vědomi skutečnosti, že budete mít povinnost vyžadovat si souhlas uživatele před samotným vydáním souborů cookies?



Komentáře firem:

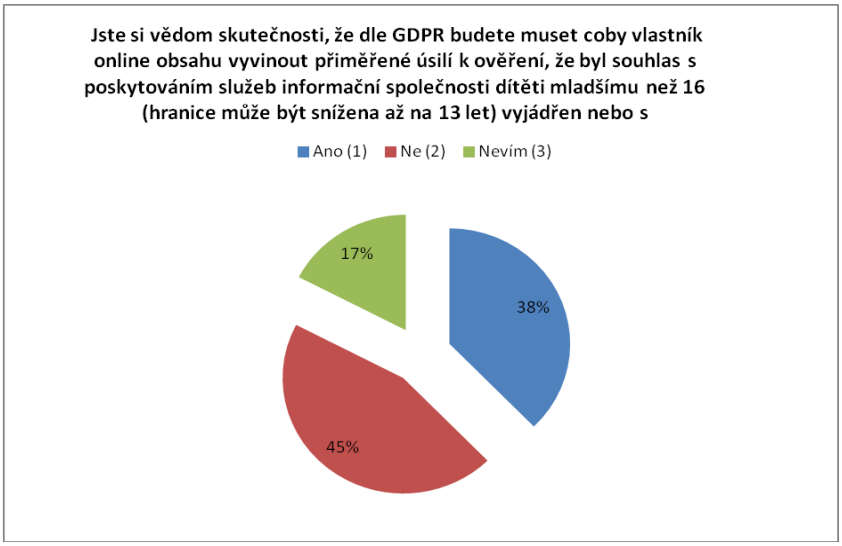
- Naše firma je běžným uživatelem internetu, e-mailové pošty firemního informačního systému a obchodní elektronické komunikace. Nemůžeme mít ani tušení, co se s mnohými daty na síti děje.
- Netýká se nás.

12c) Jste si vědomi toho, že za porušení základních zásad pro zpracování osobních údajů (včetně vydání cookies bez předchozího souhlasu uživatele, pokud tato ve spojení s jinými informacemi může identifikovat či učinit identifikovatelnou fyzickou osobu) vám hrozí pokuta až do výše 20 mil. EUR, nebo 4% celkového ročního obratu celosvětově?



13. DĚTI DO 13 LET VĚKU

13a)Jste si vědom skutečnosti, že dle GDPR budete muset coby vlastník online obsahu vyvinout přiměřené úsilí k ověření, že byl souhlas s poskytováním služeb informační společnosti dítěti mladšímu než 16 (hranice může být snížena až na 13 let) vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost?

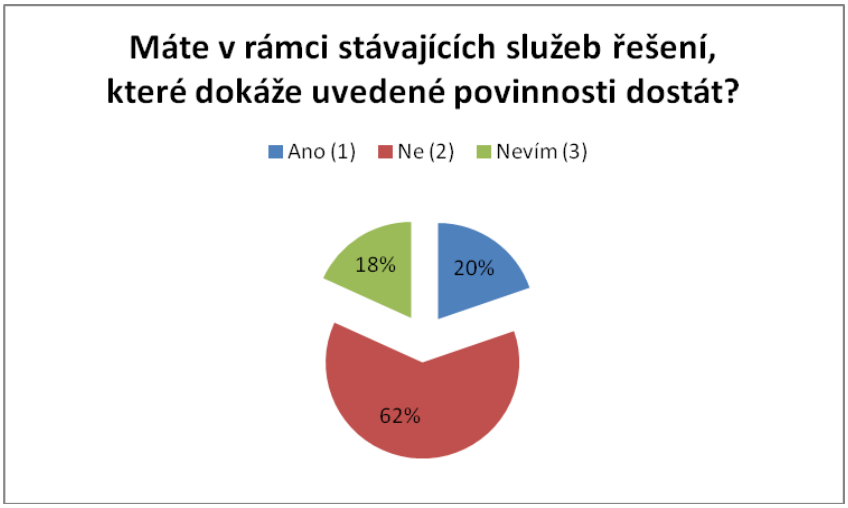


Komentáře firem:

- Co chtějí tvůrci dosáhnout? Zničit malé a střední podnikání v Evropě - mám pocit, jako bych četl nějaký absurdní, zrůdný sci-fi román.
- Netýká se nás.
- Po přečtení otázky již ano.

- S trochou ironie konstatuji, že je tím konečně autoritativně stanovena hranice cenové škály osobních údajů.

13b) Máte v rámci stávajících služeb řešení, které dokáže uvedené povinnosti dostát?



Komentáře firem:

- Nedokážeme si představit, jak technicky zabezpečit.
- Netýká se nás.
- Netýká se naší společnosti.
- V procesu.

14. MÁTE ZÁJEM O NOVINKY O VÝVOJI NEBO SE CHCETE ZAPOJIT DO PRACOVNÍ SKUPINY SP ČR PRO OCHRANU DAT?

Máte zájem o novinky o vývoji nebo se chcete zapojit do Pracovní skupiny SP ČR pro ochranu dat? Zanechte nám svůj e-mail!

- 26 firem mělo zájem o další informace
- 3 explicitně sdělily ne

Komentáře firem:

- Svoje úsilí musím věnovat tomu, aby naše firma prosperovala a aby o práci nepřišlo našich 80 zaměstnanců. Na podobné absurdity opravdu nemám čas, ale děkuji za nabídku.

ZÁVĚR

Na dotazník celkem odpovědělo více než 200 (přesně 209) firem, přičemž výstupy lze zrekapitulovat následovně:

- Přetrvávají otazníky nad řadou termínů a nejasností: jaký bude výklad ustanovení GDPR? Které povinnosti a konkrétně pro které firmy budou platit?

- Ne všichni respondenti vnímají nové povinnosti jako skutečně závazné, je proto třeba věnovat mimořádnou pozornost osvětě, zvyšování informační úrovně a právního povědomí firem a úzké komunikaci s nimi.
- Firmy v řadě případů nejsou vůbec s to odhadnout finanční náklady související se zavedením nových povinností a nebo jsou jejich odhady velmi podhodnocené (např. náklady na zavedení jednotlivých povinností v řádech desítek tisíc Kč považujeme za velmi střízlivé).

V návaznosti na výstup dotazníku Svaz průmyslu a dopravy ČR vyhodnotil situaci a na nadcházející období (první půle r. 2017) plánuje následující aktivity:

- Další rozšíření rozsahu členů Pracovní skupiny pro ochranu dat fungující v rámci Expertního týmu pro digitální ekonomiku s cílem navázat úzké diskuze s relevantními odborníky z firem na pracovní úrovni v co nejširším rozsahu,
- Pokračování aktivních diskuzí a konzultací na národní úrovni, a to zejména v rámci Pracovní skupiny Úřadu vlády pro legislativu v oblasti ochrany dat s účastí Úřadu vlády a týmu koordinátora digitální agendy ČR, Ministerstva vnitra ČR jako gestora legislativního řešení pro implementaci GDPR na národní úrovni a Úřadu pro ochranu osobních údajů jako perspektivního dozorového úřadu,
- Pokračování v diskuzích na evropské úrovni, a to jak s Evropskou komisí, tak i s tzv. Article 29 Working Party, která je perspektivním Data Protection Board,
- Osvěta a šíření povědomí o novinkách mezi firmami, a to zejména prostřednictvím:
    - Webu www.spcr.cz, svazového elektronického týdeníku SP Info a tištěného dvouměsíčníku SPEKTRUM, partnerských médií (Hospodářské noviny), mezi členskými firmami na interních jednáních Představenstva SP ČR, Rady členů a Grémia členských firem a mezi nečlenskými firmami prostřednictvím expertních vstupů a prezentací zástupců Svazu na konferencích, seminářích a diskusních fórech s podnikateli,
    - Série regionálních diskusních fór s firmami k tématu GDPR (konaných v rámci projektu NORD v období únor – březen 2017 v celkem 6 krajských městech ČR),
    - Komunikace tématu GDPR jako právního úskalí hladké implementace tzv. Průmyslu 4.0 v rámci všech souvisejících aktivit.

Kontakt pro další spolupráci:

Mgr. TEREZA ŠAMANOVÁ
manažerka pro digitální ekonomiku

SVAZ PRŮMYSLU A DOPRAVY ČR
Sekce hospodářské politiky
Freyova 948/11 | 190 00 Praha 9

Tel: 225 279 603 | GSM: 723 074 150
tsamanova@spcr.cz| www.spcr.cz

Praha, 13. ledna 2017