Grant Thornton
An instinct for growth™

GDPR Quick Check - Klient
Business Unit Profile

ID	BU01
Jméno organizace	Klient
Kontaktní osoba	
Datum zprávy	22.11.2017

Povinné otázky: 35
Dokončeno: 0
VE ZPRACOVÁNÍ

Organizace		**Odpověď**
Obecné		
D_A_01	Posouzení - Do jaké míry je ve vztahu k Vašemu odvětví v současnosti prováděna kontrola ochrany osobních údajů dozorovým orgánem (ÚOOÚ)?	
D_A_02	Posouzení - Které změny vzhledem k zavedení GDPR plánujete učinit nebo jste již učinili?	
D_A_03	Posouzení - Jak hodnotíte citlivost Vašich zákazníků na ochranu osobních údajů?	
D_A_04	Kolik má Vaše organizace celkově zaměstnanců?	
D_A_05	Kolik zaměstnanců se pravidelně zabývá zpracováním nebo používáním osobních údajů ve vaší organizaci?	
D_A_06	Ve kterém odvětví působí Vaše organizace?	
D_A_07	Má Vaše organizace další organizační složky uvnitř, případně mimo Vaši zemi?	
D_A_08	Má Vaše organizace právně nezávislé části uvnitř, případně mimo Vaši zemi?	
Odpovědnosti		0
D_A_09	Byla ve Vaší společnosti určena osoba odpovědná za ochranu dat?	
D_A_10	Outsourcovali jste služby personálního oddělení a nebo management lidských zdrojů?	
Technologie		0
D_A_11	Používáte nové technologie? (např. cloudové služby, mobilní aplikace, digitální nebo biometrické podpisy, sdílení dat)?	
D_A_12	Které z následujících kategorií systémů jsou využívány ke zpracování osobních údajů? (lze zvolit více možností zároveň)	
	Zálohovací systémy	
	Archivační systémy	
	Testovací databáze (vývoj / TEST / produkce)	
	Management znalostí (Knowledge Database / databáze znalostí)	
	Správa dodavatelů (nákup a řízení poptávky)	
	Řízení zdrojů (lidské, finanční, informační)	
	Řízení zakázek (správa smluv)	
	Systém správy záznamů	
	Systém správy dokumentů	
	Systémy pro marketing a zákaznický servis	
	Cestovní a rezervační systémy (služební cesty, letenky,...)	
	Výukové/e-learningové systémy	
	Správa kmenových dat (master data)	
	Správa ID uživatelů (správa identit)	
	Řízení lidských zdrojů	
	Správa vztahů / partnerství	
	Řízení vztahů se zákazníky	
	Správa procesů	
	Správa zainteresovaných stran	
	Správa žadatelů o zaměstnání (náborové systémy)	
	Systémy kontroly a interního auditu	
	Systémy správy vztahů se zákazníky (CRM)	
	Systémy podnikového plánování zdrojů (ERP)	
	Logistika	
	Finance a účetnictví	
	Mzdy	
	Systém řízení bezpečnosti	
	Docházkový systém	
	VideoBezpečnostní kamerový systém	
	Systémy kontroly fyzického přístupu (čipové karty)	
	Incident management	
	Service desk (help-desk)	
	Ticketing-systém	
	Komunikační systémy (e-mail, Instant Messaging)	
	IP-telefony (VoIP)	
	Systémy pro nouzovou správu	
	Systémy řízení kvality	
	Řízení pracovních/technologických postupů (plánování výroby,...)	
	Správa služeb	
	Systémy profilování nebo skórování	
Zpracovatelské činnosti		
D_A_13	Kolik je ve Vaší společnosti různých organizačních jednotek (odbor, oddělení, úsek,…), které přicházejí do styku s osobními údaji?	
D_A_14	Kolik různých (podnikových) procesů v průměru existuje v jednotlivých organizačních jednotkách?	
D_A_15	Kolik odpovědných osob (garantů) pro každý podnikový proces je třeba k jeho úplnému pochopení/porozumění?	
Osvědčení		0
D_A_16	Zavedla Vaše organizace efektivní systém řízení bezpečnosti informací (ISMS)?	
D_A_17	Vlastní vaše organizace aktuální osvědčení o dodržování pravidel ochrany dat (např. ISAE 300, EuroPrise)?	

Informace o zpracovávaných údajích		**Odpověď**
Zpracovávané údaje - obecné		0
D_B_01	Používáte osobní údaje jiných organizací?	
D_B_02	Kolik subjektů údajů je zpracováváno? (uloženo v DB,...)	
D_B_03	Do jaké míry jsou zpracovávány osobní údaje ve srovnání s celkovým objemem dat?	
D_B_04	Jsou osobní údaje automaticky zpracovávány za účelem posouzení či ohodnocení určitých osobních aspektů, jako například pracovní výkonnosti, finanční situace, zdraví, osobních preferencí, zájmů, spolehlivosti, chování, místa pobytu	
D_B_05	Jsou osobní údaje zpracovávány pro statistické účely? Statistickým účelem je chápáno jakékoli shromažďování a zpracovávání osobních údajů pro statistické analýzy či vytváření statistických výstupů.	
D_B_06	Existuje systematické a rozsáhlé sledování veřejně přístupných míst (kamerový systém, monitorování přístupu k internetu)?	
D_B_07	Užíváte archivační systémy pro dlouhodobé ukládání osobních údajů?	

Grant Thornton
An instinct for growth™

GDPR Quick Check - Klient
Business Unit Profile

ID	BU01
Jméno organizace	Klient
Kontaktní osoba	
Datum zprávy	22.11.2017

Povinné otázky: 35
Dokončeno: 0
VE ZPRACOVÁNÍ

	Skupiny subjektů údajů	0
D_B_08	Pro které z následujících skupiny subjektů údajů zpracováváte osobní data? (je možné zvolit více možností zároveň)	
	Zaměstnanci	
	Zákazníci/klienti	
	Zájemci o práci	
	Dodavatelé	
	Zainteresované strany	
	Zprostředkovatelé, prostředníci, agentury	
	Akcionáři/členové představenstva	

	Kategorie dat	0
D_B_09	Které z následujících kategorií dat zpracováváte (je možné zvolit více monžností zároveň)?	
	Osobní data (např. jméno, e-mail, adresa)	
	Zvláštní kategorie osobních údajů - náboženské vyznání	
	Zvláštní kategorie osobních údajů - data týkající se zdraví	
	Zvláštní kategorie osobních údajů - data týkající se genetiky	
	Zvláštní kategorie osobních údajů - biometrická data a vlastnosti	
	Zvláštní kategorie osobních údajů - kriminální minulost (trestní rejstřík etc.)	
	Zvláštní kategorie osobních údajů - data týkající se dětí (do 16-ti let věku)	
D_B_10	Schraňujete či zpracováváte obrazová/video data?	

Tok dat		**Odpověď**
	Infrastruktura	0
D_B_11	Využíváte služby (prodej a distribuce, lidské zdroje, mzdy, účetnictví atd.) společných organizací (společné zpracování dat)?	
D_B_12	Jaké procento systémů používá centrální infrastrukturu (např. od holdingové společnosti)?	
D_B_13	Které systémy využívají centrální IT infrastrukturu (např. centrální CRM)?	
D_B_14	Spravuje Vaše organizace také IT infrastrukturu dalších organizačních složek/společností v rámci či mimo Vaši zemi?	
D_B_15	Jaké procento systémů obsahujících osobní údaje je ovlivněno nařízením GDPR uvnitř Vaší organizace (pouze systémy v rámci Vaší zodpovědnosti)?	
D_B_16	Vyměňujete osobní údaje s jinými osobami či organizacemi (např. mateřská společnost)?	
D_B_17	Jaké opatření jsou přijata pro kontrolu nestrukturovaných dokumentů (např. excel, word,...) podléhajících ochraně osobních údajů (např. přístup, šíření, ukládání)?	

	Zpracovatelé	0
D_B_18	Využíváte externích zpracovatelů pro zpracování dat?	
D_B_19	Máte externí zpracovatele, kteří mají přístup k systémům s uloženými osobními údaji (např. za účelem údržby)?	
D_B_20	Užívá Vaše společnost cloud-services?	
D_B_21	Užívá Vaše společnost externí IT-housing služby?	

Grant Thornton
An instinct for growth™

GDPR Quick Check - Klient
Controls

ID	BU01
Jméno organizace	Klient
Kontaktní osoba	0
Datum zprávy	22.11.2017

Povinné otázky: 116
Dokončeno: 0
Ve zpracování

Procesy a opatření k ochraně osobních údajů		Odpověď
QS_01	**Strategie a manuál k ochraně osobních údajů**	
D_C_01	Existuje vedením odsouhlasená strategie/politika ochrany osobních údajů?	
D_C_02	Jsou v rámci strategie/politiky formulovány cíle ochrany osobních údajů?	
D_C_03	Mohou být dotazy dozorujícího orgánu ohledně opatření na ochranu údajů zodpovězeny přímo a přiměřeně?	
QS_02	**Směrnice pro zaměstnance**	
D_C_04	Existuje vedením schválený řízený dokument (politika/směrnice) ochrany osobních údajů pro zaměstnance (uživatelská pravidla pro ochranu OÚ)?	
D_C_05	Existují směrnice pro soukromé užívání firemního vybavení (telefon, mobilní telefon, chytrý telefon, PC, laptop, internet, e-mail) a jsou tyto směrnice pravidelně kontrolovány?	
D_C_06	Existují jasná pravidla pro používání soukromých mobilních zařízení nebo ukládání soukromých údajů?	
D_C_07	Existuje politika přístupových hesel?	
D_C_08	Zavázali se všichni, kteří pracují s osobními údaji k utajení těchto údajů (např. údaje o zaměstnancích, zákaznících, dodavatelích)?	
D_C_09	Jsou nově najatí zaměstnanci ihned zavázáni k utajení údajů (NDA)?	
D_C_10	Je zajištěno, aby byli všichni návštěvníci za všech okolností doprovázeni zaměstnanci, aby se nemohli volně pohybovat bez dozoru?	
D_C_11	Která pravidla a směrnice v kontextu ochrany a soukromí OÚ má organizace již zavedené? (napsat popis)	
QS_03	**Odpovědnosti ve společnosti**	
D_C_12	Existuje osoba zodpovědná za ochranou osobních údajů? Jaký je rozsah jejích povinností?	
D_C_13	Existují v organizaci i další role a odpovědnosti v souvislosti s ochranou osobních údajů? (specialiasta na fyzickou bezpečnost, kryptografii,...)	
D_C_14	Existují odpovědnosti za zpracování OÚ v souvisejících systémech? (např. Vlastník dat, Zpracovatel,...)	
QS_04	**Činnosti zpracování**	
D_C_15	Jsou business procesy ve společnosti známé?	
D_C_16	Jsou známy procesy ve společnosti, v jejichž rámci jsou zpracovávány osobní údaje?	
D_C_17	Máte přehled informačních systémů, které zpracovávají osobní údaje (včetně rozdělení na osobní a zvláštní osobní údaje)?	
D_C_18	Máte záznamy ohledně zpracovatelských činností - účel, kategorie zpracování? (článek 30 GDPR - Záznamy o činnostech zpracování)	
QS_05	**Zpracovávané údaje**	
D_C_19	Byly určeny účel a právní titul všech zpracovatelských aktivit?	
D_C_20	Byla určena časová rozmezí, po která budou data uložena (čas vymazání)? (archivační a skartační řád)	
D_C_21	Byl určen původ všech osobních údajů (např. poskytnutí dat subjektem, třetí stranou)?	
D_C_22	Je právní titul ke zracování znám a zdokumentován pro všechny zpracovatelské činnosti?	
QS_06	**Klasifikace dat**	
D_C_23	Byla stanovena a zavedena klasifikace ochrany osobních údajů a jejich označování (např. zdravotní data, náboženské vyznání, profilování)?	
D_C_24	Byla stanovena a zavedena klasifikace a označování osobních údajů z hlediska bezpečnosti informací (např. důvěrnost, integrita, dostupnost)?	
D_C_25	Existují nějaké směrnice či pravidla pro zacházení s utajovanými údaji pro zaměstnance, zpracovatele, atd. (např. zdravotní data musí být zašifrována)?	
QS_07	**Infrastruktura/přenos dat/tok dat**	
D_C_26	Jsou definována rozhraní mezi systémy?	
D_C_27	Existují diagramy toku dat pro výměnu osobních údajů mezi systémy?	
D_C_28	Existuje dokumentace (záznamy) toků dat, které byly doposud provedeny?	
QS_08	**Transparentnost a informace k poskytnutí**	
D_C_29	Existují směrnice pro poskytování informací subjektům údajů o manipulaci s jejich osobními údaji?	
D_C_30	Jsou subjekty údajů informovány o zpracování jejich dat a jejich právech v době zpracování dat?	
D_C_31	Upravili jste svoje texty ohledně informací o ochraně OÚ pro subjekty údajů, tak aby tyto texty, které subjekty dostávají ve chvíli poskytnutí dat, odpovídaly náležitostem podle článku 13 GDPR - Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů a 14 GDPR - Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů?	
D_C_32	Jsou zainteresované strany či klienti vždy informováni o možném užití jejich OÚ pro účely marketingu?	
D_C_33	Jsou zainteresované strany či klienti vždy informováni o možném užití jejich OÚ pro účely automatizovaného rozhodování či profilování?	
D_C_34	Byly implementovány směrnice pro manipulaci/odvolání souhlasu subjektů údajů?	
D_C_35	Adaptovali jste prohlášení souhlasu pro klienty, zainteresované strany, atd. podle požadavků článku 7 - Podmínky vyjádření souhlasu a 13 GDPR (především rozšiřující informace k poskytnutí, jako je právo kdykoliv zrušit souhlas)?	
D_C_36	Jste schopni poskytnout přesvědčující legitimní evidenci (záznamy) soulasu?	
QS_09	**Analýza rizika**	
D_C_37	Provádíte analýzu rizik IT pravidelně?	
D_C_38	Zvažujete také riziko ochrany OÚ v kontextu analýzy rizik IT?	
D_C_39	Máte v organizaci zavedenu vhodnou metodu pro určení potřeby provedení posouzení dopadů na ochrany OÚ?	
D_C_40	Máte v organizaci vhodnou metodu pro hodnocení ochrany dat?	
D_C_41	Máte nějaké nástroje k provedení zhodnocení ochrany dat?	
D_C_42	Máte seznam akcí (cílů) na základě identifikovaných a ohodnocených rizik?	
QS_10	**Integrace procesu**	
D_C_43	Jak zaručujete, že se pověřená a zodpovědná osoba aktivně zapojuje do problémů ochrany OÚ?	
D_C_44	Jak zaručujete, že je ochrana dat zvažována při zavádění a změnách procesů (článek 25 GDPR - Záměrná a standardní ochrana osobních údajů)?	
D_C_45	Jak zaručujete, že nové zpracovatelské činnosti neodporují zákonům a regulacím o ochraně OÚ?	
D_C_46	Je ochrana dat uvažována během všech procesů?	
QS_11	**Procesy ochrany dat**	
D_C_47	Byly procesy k zacházení s právy subjektů dat (např. přístup, mazání, atd.) identifikovány a zdokumentovány?	
D_C_48	Jste schopni dostát právům subjektů dat včas (1 měsíc) a jak to zajišťujete?	
D_C_49	Máte ve společnosti jediné kontaktní místo pro zpracování žádostí v rámci práv subjektů údajů?	
D_C_50	Byly zavedeny nějaké procedury a vzory pro zacházení s žádostmi o právo k přístupu?	
D_C_51	Byly ve vaší společnosti definovány adekvátní skartační procedury pro bezpečné skartování elektronických dat?	
D_C_52	Jsou osobní data automaticky skartována nebo je přístup k nim automaticky omezen po vypršení periody uložení dat či ve chvíli, kdy data přestanou být nutná ve věci, za jejímž účelem byla získána?	
D_C_53	Jsou disky a fyzické dokumenty bezpečně uloženy a zničeny (např. Drtič, fyzické skartování)?	
D_C_54	Existuje technická koncepce blokování přístupu k osobním údajům? (ochrana zájmů organizace např. využití osobních údajů při důkazním řízení, vymáhání pohledávek,...)	
D_C_55	Je soulad s minimální a maximální úložnou dobou zaručen užitím technických opatření?	
D_C_56	Jsou výhrady/námitky ke zpracování dat, podané zákazníky či zainteresovanými stranami, centrálně zaznamenány a průběžně vzhodnocovány?	
D_C_57	Používají se principy minimalizace dat při zaznamenání, skladování apod. (Např. Jsou shromažďovány pouze ty údaje, které jsou potřebné v rámci účelu)?	
D_C_58	Byly implementovány směrnice a procesy nutné pro kontrolu všech přenosů dat vzhledem k jejich legální legitimaci podle GDPR?	
D_C_59	Existuje proces/postup pro poskytování dat (strukturovaná forma - přenositelnost dat)?	
D_C_60	Byly implementovány procesy zohledňující ochranu dat pro nově příchozí/odchozí zaměstnance/zúčastněné?	
D_C_61	Jak zaručujete, že je všechen relevantní přístup zablokován, když zúčastněný (např. zaměstnanec, partner, zpracovatel) ukončí kontrakt?	
QS_12	**Porušení ochrany dat**	
D_C_62	Byla zavedena opatření pro identifikaci porušení soukromí/pravidel ohledně OÚ a příslušné metody pro určení rizik a vysokých rizik ve Vaší společnosti?	
D_C_63	Zajistili jste, že v souladu s článkem 33 GDPR, můžou být porušení soukromí/pravidel ohledně dat nahlášena dohlížejícímu orgánu během (do) 72 hodin od zjištění této skutečnosti?	
D_C_64	Máte směrnice pro systematické zjišťování porušení soukromí/pravidel ohledně dat? (sběr incidentů)	
D_C_65	Máte směrnice pro systematické zacházení s případy porušení soukromí/pravidel ohledně dat? (vyhodnocování incidentů)	
QS_13	**Zpracovatelé**	

Grant Thornton
An instinct for growth™

GDPR Quick Check - Klient
Controls

ID	BU01
Jméno organizace	Klient
Kontaktní osoba	0
Datum zprávy	22.11.2017

Povinné otázky: 116
Dokončeno: 0
Ve zpracování

D_C_66	Byly definovány směrnice, kritéria a/nebo procedury pro výběr a hodnocení externích dodavatelů?	
D_C_67	Máte seznam všech zúčastněných zpracovatelů?	
D_C_68	Vedete (písemné) smlouvy se zpracovateli dat?	
D_C_69	Obsahují kontrakty, do nichž jste vstoupili společně se zpracovateli, záruky ohledně smazání/zničení dat po ukončení kontraktu, povinnosti v rámci důvěrnosti, specifikace pro sub-zpracovatele, kontraktové pokuty, právo k auditu stejně jako spolupracovní povinnosti, inspekční povinnosti a informační povinnosti?	
D_C_70	Provádíte pravidelné hodnocení společností, které zpracovávají osobní data Vaším jménem nebo které poskytují údržbu Vašich IT systémů a dokumentujete (záznamy) výsledky takových zhodnocení?	

QS_14 Vědomí a trénink

D_C_71	Existuje program vzdělávání zaměstnanců (plánované tréninkové kurzy)?	
D_C_72	Máte školicí materiály/tréninkové kurzy týkající se ochraně osobních údajů?	
D_C_73	Jsou zaměstnanci pravidelně školeni v zacházení s OÚ?	
D_C_74	Je prováděno hodnocení efektivity vzdělávání?	
D_C_75	Je dokumentována (záznamy) účast na tréninicích?	

QS_15 Audit a kontinuální zlepšování

D_C_76	Je dodržování požadavků na ochranu údajů a zabezpečení OÚ pravidelně kontrolováno z hlediska účinnosti?	
D_C_77	Je efektivita opatření k ochraně dat pravidelně reportována vedení společnosti?	

Opatření k ochraně informací		**Odpověď**
QS_16	**Obecné nároky na ochranná opatření**	
D_D_01	Jsou v podniku zavedena a zdokumentována technická a organizační opatření na ochranu a zabezpečení dat?	
D_D_02	Byly určeny možnosti anonymizace a pseudonymizace osobních dat?	
QS_17	**Bezpečnost osobní a bezpečnost prostředí**	
D_D_03	Existuje koncept fyzicky bezpečných míst (např. veřejná místa, kanceláře, datová centra, vysoko-bezpečnostní místa)?	
D_D_04	Byl omezen vstup do kanceláří za pomoci kontrolních mechanismů (např. vstupní karty, recepční)? Máte poplašný systém?	
D_D_05	Byl přístup do zpracovatelských míst/k nástrojům (např. místnosti se servery, data centra) omezen za pomoci přísných přístupových pravidel a rozšířených bezpečnostních kontrol (např. PIN kód, otisky prstů)? Je možné identifikovat, které osoby kdy měly přístup k datům?	
QS_18	**Kontrola přístupu**	
D_D_06	Existuje koncept přístupu založený na rolích/úkolech a principu "nezbytné znalosti" (need to know)?	
D_D_07	Je přístup k osobním datům podmíněn bepečnostními kontrolními mecanismy a bezpečnostními hesly (např. silná hesla, časté změny hesel)?	
D_D_08	Je počet oprávnění administrátorů omezený na minimum a jsou pravidelně kontrolování?	
D_D_09	Je přístup k osobním údajům povolen pouze po užití uživatelských profilů a osobních identifikací?	
D_D_10	Existuje postup pro zpřístupnění/znepřístupnění dat a jsou hesla předávána bezpečně?	
D_D_11	Je pro vstup ke speciálním kategoriím osobních údajů vyžadována speciální bezpečnostní kontrola (např. certifikáty, dvoufaktorová autentifikace)?	
D_D_12	Je zajištěn přístup k zálohám a kopiím dat (např. USB disk / HDD) pomocí autentizačních a šifrovacích opatření?	
QS_19	**Bezpečnost sítě**	
D_D_13	Byly systémy izolovány od externích přístupů z veřejných sítí za pomoci firewallů a podobných systémů?	
D_D_14	Byl nainstalován antivirový software, který nemůže být odstaven uživateli, jenž vynucuje pravidelný scan a reportuje podezřelé nálezy centrále? Uvažujte prosím servery, koncová zařízení a síťová zařízení.	
D_D_15	Existují nějaká pokročilá opatření pro zabezpečení sítě (např. IDS / IPS, DDOS ochrana, SIEM)?	
D_D_16	Máte síťové ochranné mechanismy, které omezují logický přístup k síťové vrstvě (např. segmentace sítí, 802.1X)?	
QS_20	**Dostupnost**	
D_D_17	Existují fyzická bezpečnostní opatření k ochraně dostupnosti (např. protipožární opatření, klimatizace, UPS, poplašný systém, protipovodňová ochrana)?	
D_D_18	Provádíte pravidelné zálohování osobních údajů?	
D_D_19	Uchováváte zálohy mimo areál společnosti nebo na bezpečném místě (geograficky oddělená záloha)?	
D_D_20	Existují záložní postupy a pravidla nahrazování kritických zdrojů (např. klíčoví pracovníci, zásadní zpracovatelé, hardware)?	
QS_21	**Bezpečnostní a nouzová opatření**	
D_D_21	Jsou používány kontroly dat (kontrolní sumy apod.) v průběhu zpracování dat, jejich přenosu nebo při tvorbě a kontrole záloh?	
D_D_22	Je implementováno logické nebo fyzické oddělení dat (např. samostatná databáze / tabulka pro každého klienta v cloudových systémech)?	
D_D_23	Je zavedeno dělení na produkční a testovací systémy stejně tak jako process řízení změn?	
QS_22	**Integrita**	
D_D_24	Jsou používány kontroly dat (kontrolní sumy apod.) v průběhu zpracování dat, jejich přenosu nebo při tvorbě a kontrole záloh?	
D_D_25	Je implementováno logické nebo fyzické oddělení dat (např. samostatná databáze / tabulka pro každého klienta v cloudových systémech)?	
D_D_26	Je zavedeno dělení na produkční a testovací systémy stejně tak jako process řízení změn?	
QS_23	**Odolnost**	
D_D_27	Existují SLA se zpracovateli a jsou definovány parametry výkonu systému?	
D_D_28	Existuje kontinuální monitorování výkonu systémů?	
D_D_29	Jsou reportovány IT incidenty a jsou vyvozována opatření proti výkonnostním problémům?	
QS_24	**Bezpečnost komunikace**	
D_D_30	Jsou dálkové přístupy (prostřednictvím veřejných sítí) chráněny silným ověřováním a šifrováním?	
D_D_31	Jsou používána silná ověřování a šifrování pro externí přenosy osobních údajů?	
D_D_32	Je pro přenos dat používána řízená komunikace (např. známá skupina příjemců pomocí e-mailu, omezení IP-adresy pro rozhraní)?	
D_D_33	Je přenos dokumentů nebo nosičů dat prováděn za použití bezpečných postupů (např. zapečetěné obálky, kurýrní služby apod.)?	
QS_25	**Šifrování**	
D_D_34	Existují požadavky na povinné použití šifrování?	
D_D_35	Je úložiště mobilních zařízení šifrována?	
D_D_36	Jsou mobilní odpojitelná média (např. USB disky) automaticky šifrována?	
QS_26	**Logování**	
D_D_37	Je přístup k osobním údajům, jejich změna apod. srozumitelně zdokumentován a zaznamenán (log) na základě přiřazených osobních uživatelských účtů?	
D_D_38	Existuje ochrana přístupu k datům protokolů (např. čtení pouze pro autorizované administrátory) a je analýza logů možná pouze na základě definovaných pravidel (např. zásada "čtyř očí" s účastí DPO, vedoucího HR nebo IT)?	
D_D_39	Existují protokoly (logy) o provedených automatizovaných přenosech dat?	