squalio

GDPR IT audits / novērtējums

SATURS

1. IEVADS 2
2. KOPSAVILKUMS 3
   2.1. Risku novērtējuma pārskats un metodoloģija 3
   2.2. Atklāto risku apkopojums 4
3. PIELIKUMI 5
   3.1. Risku detalizēts apraksts un ieteikumu uzskaitījums 5
   3.2. IT labās prakses izklāsts 8
   3.3. Atbildības ierobežojums 9

1. IEVADS

Atskaite ir sagatavota SQUALIO sniegtajam pakalpojumam "GDPR IT Audits" un ieķļauj risku pārskatu, kas saistīti ar IT drošību un atbilstību Vispārējai datu aizsardzības regulai (GDPR, Regula). Atskaite satur potenciālo risku kopsavilkumu, detalizētu risku aprakstu, rekomendācijas un risinājumu ieteikumus atklāto risku mazināšanai.

Pakalpojums sniegts klientam:	**SIA "XX"**
Uzsākšanas datums:	**2018. gada XX. maijs**
Atskaites iesniegšanas datums:	**2018. gada XX. maijs**

GDPR IT Audits ir balstīts uz informāciju, ko klients ir iesniedzis SQUALIO, izmantojot elektronisku tiešsaistes aptauju un veicot datorsistēmu inventarizāciju. Visa klienta sniegtā informācija ir atspoguļota pielikumā. Novērtējuma laikā riski tiek identificēti, vadoties pēc SQUALIO izstrādātas risku novērtēšanas metodoloģijas, kas iekļauj IT procesu drošības novērtējumu un atbilstību regulai. GDPR IT Audita process tiek veikts, sekojot 3 soļiem:

1) **Tiešsaistes anketas aizpildīšana**. Elektroniskā tiešsaistes anketas aizpildīšana par uzņēmumu, izmantotajiem IT risinājumiem un uzņēmuma ikdienas darbu ar personu datiem;
2) **Datorsistēmu inventarizācija.** IT sistēmu inventarizācija, izmantojot automatizētu datoru inventarizācijas rīku SNOW Software. Inventarizācijas laikā uz **XX** uzņēmuma datoriem tiks uzstādīts skenēšanas aģents un iegūts pārskats par datoros esošo programmatūru un tās lietojumu;
3) **Atskaites sagatavošana**. SQUALIO, balstoties uz pakalpojuma laikā iegūtajiem datiem, veic risku analīzi IT drošībai un atbilstībai regulai un sagatavo pakalpojuma atskaiti.

GDPR IT Audita atskaite sastāv no sekojošām daļām:

- Kopsavilkums ar atklāto risku apkopojumu;
- Pielikums ar detalizētu risku skaidrojumu, ieteikumiem risku novēršanai un IT labo praksi;
- Pavadošais izklājlapas dokuments ar pakalpojuma laikā ievāktajiem datiem.

2. KOPSAVILKUMS

2.1. Risku novērtējuma pārskats un metodoloģija

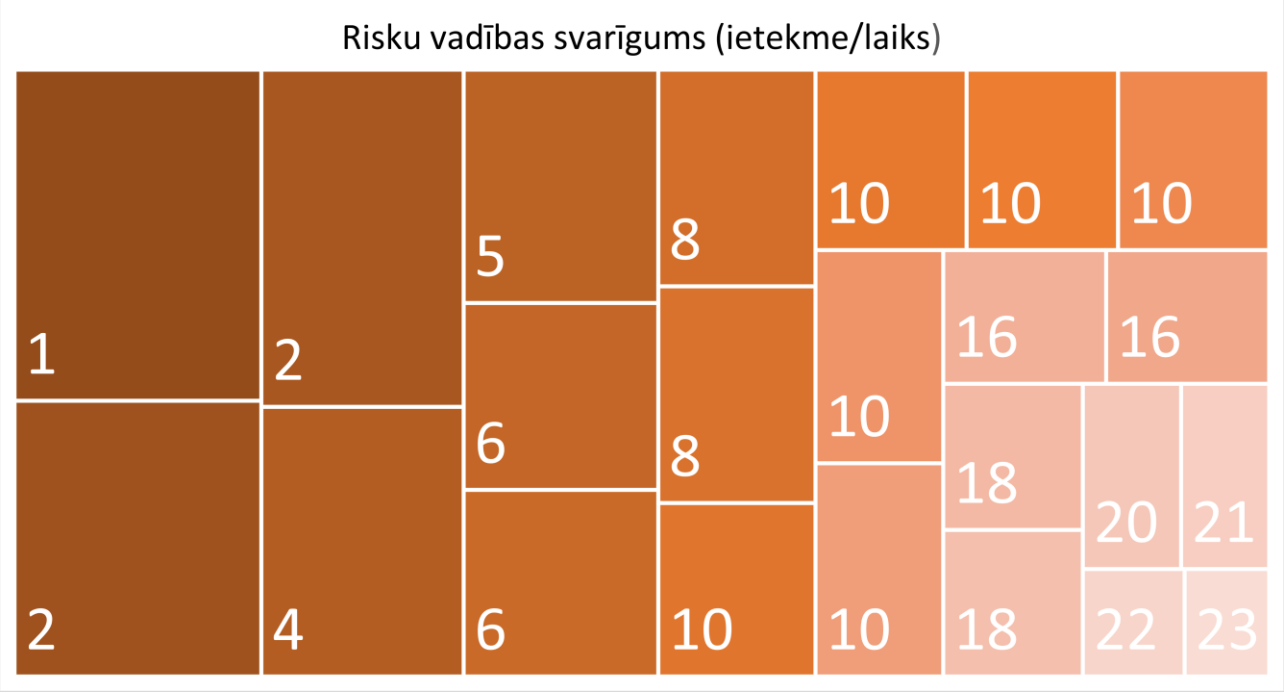
GDPR IT Audita laikā kopumā tika identificēti XX riski, kas ir saistīti ar IT drošību un kontroli attiecībā uz vispārējo datu aizsardzības regulu. Lai novērtētu prioritāros riskus, visiem GDPR IT Audita laikā identificētajiem riskiem tika noteikts riska svarīguma koeficients - augstākam riska svarīguma koeficientam ir piemērota augstāka riska prioritāte. Riska svarīgums ir aprēķināts, izmantojot sekojoša formulu:

$$Riska\ svarīgums = \frac{Riska\ radītā\ ietekme}{Riska\ novēršanai\ nepieciešamais\ laiks}$$

Riska svarīguma aprēķinā izmantotā riska ietekmei un riska novēršanai nepieciešamais laiks ir SQUALIO ekspertu piešķirta vērtība skalā no 1 līdz 5, katram no atklātajiem riskiem.

- Riski, kam ir piešķirta augstāka prioritāte, rada lielāku ietekmi un to atrisināšanai nepieciešams īsāks laiks;
- Riskam(-iem) ar 1. prioritāti ir visaugstākais svarīguma koeficients;
- Ja vairākiem riskiem ir noteikts vienāds svarīguma koeficients, tad tie ir atspoguļoti grafikā ar identisku prioritātes numuru;
- Riskus ar augstāku prioritāti ieteicams atrisināt pirmos.

Visi identificētie riski un to prioritātes pārskats ir ilustrēts zemāk pievienotajā grafikā “Risku vadības svarīgums”.



2.2. Atklāto risku apkopojums

Tabulā 2.1 ir uzskaitīti visi atklātie riski un to prioritāte, kas tika noteikta, izmantojot aprakstīto risku novērtēšanas metodoloģiju.

Tabula 2.1. Atklāto risku pārskats

Nr.	Riska nosaukums	Prioritāte risku pārskatā
1.	Nespēja nodrošināt regulas prasībām atbilstošu datorlietotāju kontroles līmeni	1
2.	Sarežģīti kontrolējams datu noplūdes un glabāšanas neatbilstības risks	2
3.	Risks neatgriezeniski zaudēt uzņēmuma datus ļaunprātības vai negadījuma dēļ	2
[..]	[..]	[..]

3. PIELIKUMI

3.1. Risku detalizēts apraksts un ieteikumu uzskaitījums

Tabula 2.1. Risku apraksts un risinājumi

Nr.	Risks	IT riska skaidrojums	GDPR riska skaidrojums	Riska mazināšanas pasākums/-i	Ieteicamais tehniskais risinājums/-i
1.	Nespēja nodrošināt regulas prasībām atbilstošu aizsardzības līmeni	Neieviešot centralizētu datorlietotāju un paroļu pārvaldības mehānismu ir ļoti sarežģīti un laikietilpīgi pārvaldīt uzņēmuma lietotājus, tādēļ parasti šādos gadījumos tiek izmantoti noklusēti lokālie lietotāji (User, Administrator, Admin), kas datu noplūdes gadījumā noved pie neidentificējama lietotāja un parolēm, kuras ir viegli uzminamas/atlaužamas, tāpat nereti darbinieka noklusētajam kontam tiek piešķirtas administratora tiesības, kas būtiski atvieglo ļaunprātīgas programmatūras (vīrusu, trojas zirgu, kriptovīrusu, u.c.) iekļūšanu un izplatīšanos sistēmā, kas savukārt tālāk noved pie datu noplūdes.	Active directory ir viens no mehānismiem, kas ļauj apstrādāt datus tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus. Šāda mehānisma neizmantošana noteiktā situācijā var tikt interpretēta kā nepietiekoša aizsardzības līmeņa nodrošināšana, dēļ kā datu pārzinis vai apstrādātājs var tikt saukts pie atbildības. **Saistītie Regulas panti: 24.pants; 25.pants; 28.pants; 32.pants.**	Jāievieš centralizēts lietotāju un paroļu risinājums, kā arī jāizveido uzņēmuma datorsistēmu paroļu politika atbilstoši kompānijas IT drošības politikai. Nokonfigurēt paroļu politikas atribūtus (lielie burti, mazie burti, simboli, cipari, to, cik reizes iespējams ievadīt paroli nepareizi pirms konts tiek aizbloķēts, to, cik bieži parole ir jāmaina, u.c.). Tāpat, izmantojot aktīvās direktorijas drošības grupas detalizēti jāizdala, katra lietotāja tiesības datorsistēmā/-ās un citos IT resursos, lai jebkurā brīdī varētu izsekot konkrētā lietotāja piekļuves līmenim tajos. Kā nākamais no veicamajiem risku samazināšanas pasākumiem ir grupu politikas/-ku izveide un definēšana, kas nosaka konkrētus drošības iestatījumus darbinieku datorsistēmām.	Ieviest kādu no centralizētiem lietotāju un paroļu pārvaldības risinājumiem: 1) Uzstādīt Microsoft Windows Server un ieviest aktīvo direktoriju (Piezīme: Gala lietotāja iekārtai nepieciešams Windows 7 Pro vai labāks); 2) DC/DNS servera lomas uzstādīšana, grupu(-as) politikas(-u) ieviešana; 3) Papildināt ar Azure AD + Intune risinājumu, konfigurēt Intune politiku gala iekārtām (Piezīme: Gala lietotāja iekārtai nepieciešams Windows 10 Pro vai labāks)

Nr.	Risks	IT riska skaidrojums	GDPR riska skaidrojums	Riska mazināšanas pasā-kums/-i	Ieteicamais tehniskais risinājums/-i
2.	Sarežģīti kontrolējams datu noplūdes un glabāšanas neatbilstības risks	Darbinieki, kuriem darba vajadzībām nebūs pieejams ērts un ātrs failu apmaiņas risinājums starp darba kolēģiem, klientiem un sadarbības partneriem, šo funkciju atradīs privātajos risinājumos, piemēram, Failiem.lv, DropBox Personal, WeTransfer, u.c. Šādu risinājumu izmantošana gala rezultātā rada datu noplūdes risku, jo uzņēmumam nav tehniskie risinājumi, lai aizsargātu šos datus un pienācīgi pārvaldītu tos. Darbiniekam atstājot uzņēmumu, šie dati "tiek paņemti līdzi" privātajos failu apmaiņas pakalpojumos.	Neieviešot drošu korporatīvo failu apmaiņas risinājumu, datu noplūdes gadījumā darbinieku saziņa privātajos risinājumos tiks novērtēta kā nepietiekošs datu aizsardzības kopējais risinājums un uzņēmums tiks saukts pie atbildības par neefektīvu IT drošības sistēmu, kas citā starpā ne tikai ļauj trešajām personām piekļūt datiem bez datu subjekta piekrišanas uz to, bet arī liedz datu subjektam realizēt savas tiesības tikt aizmirstam. **Saistītie Regulas panti: 5.panta 1(b).punkts, 1(f).punkts; 17.pants; 24.pants; 25.pants; 28.pants; 32.pants.**	Ieviest centralizētu failu apmaiņas risinājumu, kuru iespējams savietot ar centralizētu paroļu pārvaldības risinājumu, lai brīdī, kad darbinieks pārtrauc darba attiecības, pāris sekunžu laikā būtu iespējama piekļuves liegšana esošo failu lejupielādei. Tāpat šada risinājuma gadījumā būs tehnoloģiski iespējams detalizēti definēt piekļuves tiesības dažādiem resursiem.	Ieviest kādu no centralizētiem failu apmaiņas risinājumiem: 1) OneDrive for Business, pieejams ar Office 365 vai patstāvīgi, piemērots lielizmēra failiem; 2) SharePoint Online, pieejams ar Office 365 vai patstāvīgi, ērts projektveida dokumentiem; 3) Windows Server ar FileServer lomu, ja uzņēmumā ir pieejama sava serveru infrastruktūra.

Nr.	Risks	IT riska skaidrojums	GDPR riska skaidrojums	Riska mazināšanas pasākums/-i	Ieteicamais tehniskais risinājums/-i
3.	Risks neatgriezeniski zaudēt uzņēmuma datus ļaunprātības vai negadījuma dēļ.	Lai nodrošinātos pret datu zudumu iekārtu nekorektu darbību rezultātā, nepieciešams ieviest vienotu rezerves kopiju risinājumu, kas nodrošinās periodisku rezerves kopiju izveidi IT sistēmām.	Saskaņā ar Regulā noteikto, uzņēmumam ir pienākums nodrošināt, ka personas dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša datu drošība, tostarp aizsardzība pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus. Līdz ar to, ieviešot vienoto rezerves kopiju risinājumu, tiks ievērots viens no Regulā noteiktajiem obligātajiem datu apstrādes principiem - "integritāte un konfidencialitāte". **Saistītie Regulas panti: 83.apsvērums; 4.panta 12.punkts; 5.panta 1(f).punkts; 24.pants; 25.pants; 28.pants; 32.pants.**	Ieviest vienotu rezerves kopiju risinājumu, kas nodrošinās periodisku rezerves kopiju izveidi IT sistēmām. Veikt periodisku rezerves kopiju atskaiti (report), kurā tiek attēlotas visas veiksmīgi izveidotās un neveiksmīgi veidotās rezerves kopijas. Periodiski veikt pārbaudi, lai pārliecinātos par rezerves kopijas korektumu.	Ieviest rezerves kopiju risinājumu: 1) Veeam, pielāgojams visdažādākajiem scenārijiem; 2) Azure Backup & Site Recovery, vienkārši lietojams reizē ar citiem Azure servisiem; 3) Files.fm Backup, vienkārši lietojams, pieejams datucentrs Latvijā.

3.2. IT labās prakses izklāsts

Tablula 3.2. IT labās prakses izklāsts

Nr.	Nosaukums	IT labā prakses apraksts	Saistītie Regulas punkti
1.	Datorlietotāju un to paroļu pārvaldība	Nepieciešams pārskatīt uzņēmuma datorsistēmu paroļu politiku atbilstoši kompānijas IT drošības politikai. Jānokonfigurē paroļu politikas atribūtus (lielie burti, mazie burti, simboli, cipari, to, cik reizes iespējams ievadīt paroli nepareizi pirms konts tiek aizbloķēts, to, cik bieži parole ir jāmaina, u.c.). Tāpat, izmantojot aktīvās direktorijas, drošības grupas detalizēti jāizdala, katra lietotāja tiesības datorsistēmā/-ās un citos IT resursos, lai jebkurā brīdī varētu izsekot konkrētā lietotāja piekļuves līmenim tajos. Kā trešais no veicamajiem risku samazināšanas pasākumiem ir grupu politikas/-ku izveide un definēšana, kas nosaka konkrētus drošības iestatījumus darbinieku datorsistēmām.	24.pants; 25.pants; 28.pants; 32.pants
2.	Darbinieku piekļuves kontrole IT resursiem	Veikt esošo lietotāju auditu centralizētajā lietotāju un paroļu risinājumā, lai pārliecinātos, ka tur nav aktīvi darbinieku konti, kas pārtraukuši darba attiecības. Pārskatīt uzņēmuma IT sistēmas un to piekļuves izveidošanas/bloķēšanas procesu, definēt bloķēšanas politiku un pārbaudes mehānismu, kas novērš iespēju neeksistējoša darbinieka lietotāju atstāt aktīvu pēc darba attiecību pārtraukšanas.	5.panta 1(f).punkts; 24.pants; 25.pants; 28.pants; 32.pants
3.	Piekļuve IT sistēmām un failiem	Veikt darbinieku izglītošanu un apmācību, kurā tiek skaidrota ietekme uz nedrošu paroļu izmantošanu un glabāšanu.	5.panta 1(f).punkts; 24.pants; 25.pants; 28.pants; 32.pants
[..]	[..]	[..]	[..]

3.3. Atbildības ierobežojums

Izpildītāja Novērtējuma saturs tiek sniegts un ir saistīts tikai ar to informāciju un tiem pieejas datiem, ko Uzņēmums ir Izpildītājam iesniedzis un/vai nodrošinājis, tāpēc Novērtējumā iekļautā un mutiski sniegtā informācija, ko Izpildītājs sniedz Uzņēmumam, nevar tikt attiecināta pilnībā uz visiem Uzņēmuma organizatoriskiem, VDAR atbilstības un informācijas sistēmu un/vai iekārtu un/vai licenču trūkumiem, un tiem piemērojamiem risinājumiem.

Padarot pieejamu Novērtējumu un saistītās dokumentācijas saturu Uzņēmumam, sniedzot atzinumu par to, Izpildītājs dalās ar savu viedokli un praksi par piemērojamību un veicamām darbībām, lai nodrošinātu drošu personas datu apstrādi saskaņā ar Regulas prasībām.

Tāpat ir būtiski ņemt vērā, ka:

- neviens nosacījums netiek tieši vai netieši izvirzīts, kā arī netiek sniegtas garantijas tieši vai netieši par Novērtējuma pilnu atbilstību Uzņēmuma sistēmu, licenču un to lietojumu situācijai;
- Izpildītājs un tā darbinieki, kā arī Izpildītāja Pakalpojumu sniegšanā piesaistītās trešās personas neuzņemas nekādu atbildību par Novērtējuma izmantošanu vai informāciju, ko sniedzis Izpildītājs, kā arī par to sniegtajiem materiāliem vai dokumentiem. Izpildītāja sniegtā informācija balstās uz jaunāko zinātnisko informāciju par VDAR atbilstības metožu un atbildības izpratni Novērtējuma sagatavošanās dienā. No brīža, kad Uzņēmums ir saņēmis Pārskatu un papildu padomu, atbildību par Uzņēmumam sniegto dokumentu un informācijas izmantošanu pilnībā uzņemas Uzņēmums;
- ja mainās izpratne un informācija par VDAR atbilstības metožu un atbildības izpratni, tad Izpildītājs neuzņemas atbildību par Uzņēmumam sniegtiem dokumentiem;
- gan Izpildītājs un tā darbinieki, gan Izpildītāja Pakalpojumu sniegšanā piesaistītās trešās personas tiek pilnībā atbrīvotas no atbildības par to, kā Klients tālāk izmanto Pakalpojumu nodevumus un jebkādus Izpildītāja un tā piesaistīto trešo personu sniegtos padomus vai informāciju. No Pakalpojumu saņemšanas brīža Klients ir pilnībā atbildīgs par turpmākajām ar Pakalpojumu nodevumiem veiktajām darbībām;

Gadījumā, kad Pārskatā ir identificēti un ietverti riski, tai skaitā attiecībā uz trūkumiem datu apstrādes un glabāšanas sistēmās un pieejās, par ko Uzņēmums nav sniedzis informāciju Pakalpojumu sniedzēja veiktās revīzijas vajadzībām, Uzņēmums uzņemas visu atbildību par profesionālu sistēmas uzlabojumu, procesu grafiku un kontroles ieviešanu, kā arī par regulāru risku novērtējumu veikšanu un pieļaujamo risku pakāpju noteikšanu, un risku mazināšanas darbību īstenošanu, kas atbilst konkrētai Uzņēmuma uzņēmējdarbībai.