LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

VISPĀRĪGAS DATU AIZSARDZĪBAS REGULAS PIELIETOJUMA APSKATS STARPTAUTISKĀ IT UZŅĒMUMĀ

BAKALAURA DARBS

Autors: **Katerīna Verdiša**
Studenta apliecības Nr.: kv15015
Darba vadītājs: profesors, Dr.dat. Māris Vītiņš

RĪGA 2019

ANOTĀCIJA

2018. gada 25. maijā spēkā stājās Vispārīgā datu aizsardzības regula, kuras mērķis ir padarīt datu drošības regulējumu atbilstīgu mūsdienu tehnoloģijām. Regulas ieviešana attiecas uz visiem uzņēmumiem, kas nodarbojas ar datu glabāšanu un apstrādi, tostarp arī IT uzņēmumiem.

Galvenā lieta, kas saista uzņēmēju uzmanību, ir sankcijas par regulas noteikumu pārkāpumiem. Lai samazinātu šo risku, uzņēmumā nepieciešams veiksmīgi implementēt regulas noteikumus, tāpēc ir jāizveido vadlīnijas, kas atvieglotu šo procesu.

Aprakstošā metode tika pielietota, lai izpētītu regulas būtību, tās nosacījumus, vēsturisko tapšanu un pielietojuma nepieciešamību IT uzņēmumā.

Analītiskā metode un salīdzinošā analīze tika pielietota, lai analizētu situāciju izvēlētajā starptautiskajā IT uzņēmumā, salīdzinātu to ar regulas prasībām un ar situāciju, kas bija pirms tās stāšanās spēkā, kā arī izveidotu vadlīnijas, kas veicinātu uzņēmuma darbības atbilstību regulai.

Darbā tika konstatētas dažas problēmas ar regulas pielietojumu uzņēmumā un tika piedāvātas vadlīnijas un apmācību materiāli.

Atslēgas vārdi: Vispārīgā datu aizsardzības regula, VDAR, personas dati, datu drošība, vadlīnijas

ABSTRACT

OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION IMPLEMENTATION IN AN INTERNATIONAL IT COMPANY

On May 25, 2018, the General Data Protection Regulation became enforceable, aimed at making data security regulation consistent with modern technologies. The implementation of the regulation applies to all companies involved in data storage and processing, including IT companies.

The main thing that draws the attention of entrepreneurs is sanctions for violations of the regulation. In order to reduce the risk, it is necessary to successfully implement the conditions of the regulation in the company, therefore, guidelines should be created to facilitate this process.

The descriptive method was used to study the essence of the regulation, its conditions, historical development and the necessity for its use in an IT company.

The analytical method and comparative analysis were used to analyze the situation in the selected international IT company, compare it with the requirements of the regulation and the situation prior to its enforcement, as well as to develop guidelines to facilitate the compliance of the company with the regulation.

Some problems with the application of the regulation were identified in the company, and guidance and training materials were provided.

Keywords: General Data Protection Regulation, GDPR, personal data, data security, guidelines

SATURA RĀDĪTĀJS

APZĪMĒJUMU SARAKSTS

API – Application Programming Interface – lietojumprogrammas saskarne.

CMS – Content Management System – satura vadības sistēma - programmatūra, kas ļauj vairākiem lietotājiem vienlaikus izveidot, apstrādāt un organizēt dažāda veida dokumentus.

CNIL – Commission nationale de l'informatique et des libertés – informatizācijas un brīvības nacionālā komisija.

Cookies – cepums jeb sīkdatnes – neliels datu fragments, ko izmantotais tīmekļa serveris nosūta lietotājam uz viņa datoru.

CRM – Customer Relations Management – klientu attiecību pārvaldība – sistēma, kas palīdz organizācijām automatizēti pārvaldīt attiecības ar klientiem.

CV – Curriculum Vitae – dzīves apraksts – dokuments, kura autors sniedz informāciju par saviem datiem, izglītību, darba pieredzi un zināšanām, kas bieži tiek iesniegts potenciālajā darba vietā.

Datu apstrāde – darbības ar personas datiem, tādas kā datu vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana.

Datu pārzinis – fiziska vai juridiska persona, aģentūra, publiska iestāde vai cita struktūra, kas individuāli vai kopīgi ar citām nosaka personas datu apstrādes mērķus un metodes.

Datu subjekts – fiziska persona, kurai pieder personas dati.

ES – Eiropas Savienība.

Git repozitorijs – versiju kontroles sistēma.

Gmail – Google organizācijas piedāvātais bezmaksas tīmekļa e-pasts.

HTML – HyperText Markup Language – iezīmēšanas valoda, ko bieži izmanto tīmekļa lapu izveidē.

IP – intertīkla protokols.

IT – informācijas tehnoloģijas.

JSON – JavaScript Object Notation – formāts, kas radās no JavaScript valodas, bet tiek uzskatīts par no valodas neatkarīgu formātu un var tikt izmantots jebkurā citā programmēšanas valodā.

MS SharePoint – Microsoft SharePoint – ir produkts, ko organizācija izmanto kā drošu vietu, kur var glabāt, organizēt, koplietot informāciju un piekļūt tai no jebkuras ierīces visiem darbiniekiem.

Open source – atvērta piekļuve sistēmas pirmkodam.

Opt-in – iestāšanās izvēles princips.

Opt-out – izstāšanās izvēles princips.

Personas dati – informācija, kas attiecas uz identificētu vai identificējamu fizisko personu.

PIA – privacy impact assessment – privātuma ietekmes novērtējums – process, kas palīdz uzņēmumiem identificēt un samazināt datu drošības riskus.

Pikšķerēšana – ļaunprātīgs krāpšanas veids internetā, kura mērķis ir ar viltu iegūt lietotāja konfidenciālo informāciju.

Postman – API testēšanas rīks.

Pseidonimizācija – personas datu apstrādes metode, kuru pielietojot personas dati kļūst neatpazīstami un tos nevar piesaistīt konkrētai personai bez papildu informācijas.

Sensitīvie dati – īpaša datu kategorija, kas norāda personas rasi, etnisko izcelsmi (tautību), reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi.

Single sign-on – vienotā pierakstīšanās – tas ir lietotāja autentifikācijas process, kura laikā persona var izmantot vienus datus, pieslēdzoties dažādām sistēmām vai lietotnēm.

UI – User interface – lietotāja saskarne – programmatūras vai sistēmas līdzekļu kopums, kas nosaka lietotāja iespējas sadarboties ar datoru.

VDAR – Vispārīgā datu aizsardzības regula.

IEVADS

Šobrīd datu drošība ir viens no aktuālākajiem tematiem. Pēdējo gadu laikā ir strauji mainījies to apstrādes un glabāšanas veids, un lietotāji nereti interneta vidē labprātīgi atstāj savus personas datus, neaizdomājoties par sekām. Sakarā ar to ir mainījusies arī datu vērtība un nozīme.

Lai datu drošības tiesiskais regulējums atbilstu mūsdienu tehnoloģijām, kas apstrādā un saglabā personas datus, 2018. gada 25. maijā stājās spēkā Eiropas Savienības Vispārīgā datu aizsardzības regula. Tā pasargā Eiropas Savienības dalībvalstu iedzīvotāju datus, pieprasot, lai datu apstrādes mērķi būtu saprotami katram. Ja organizācijas nebūs spējīgas ievērot regulas prasības, tās gaida bargi naudas sodi.

Pēc regulas nosacījumiem katram uzņēmumam, kas nodarbojas ar ES iedzīvotāju datu apstrādi un drošību, ir jāatbilst regulas prasībām.

Darba mērķis ir izpētīt regulas ieviešanu un pielietojumu starptautiskā IT uzņēmumā, salīdzināt, ar ko tās implementācija atšķiras no implementācijas vienkāršā komercuzņēmumā, izveidot vadlīnijas ar ieteicamajiem rīkiem, kas varētu atvieglot regulas ievērošanu, un apskatīt pašreizējo situāciju ar datu drošību uzņēmumā un tā izmantoto rīku.

Lai sasniegtu šo mērķi, jāveic šādi uzdevumi:

- Izpētīt VDAR būtību, nosacījumus, tās aizsargātos datus un ieviešanas nepieciešamību.
- Salīdzināt datu aizsardzības tiesisko regulējumu Latvijas Republikā pirms un pēc VDAR ieviešanas.
- Izpētīt VDAR nepieciešamību IT uzņēmumā un salīdzināt, kā mainījusies situācija gadu pēc regulas ieviešanas.
- Izstrādāt vadlīnijas veiksmīgai VDAR implementēšanai IT uzņēmuma darbībā.
- Izpētīt un ieteikt uzņēmumam VDAR atbalsta rīku.
- Analizēt izvēlētā rīka darbību.

Šīs darbs sastāv no septiņām daļām:

Pirmajā daļā tiek apskatīta Vispārīgā datu aizsardzības regula, tās ieviešanas nepieciešamība, nosacījumi un aizsargājamā datu subjekta tiesības.

Otrā daļa apskata regulas pielietojumu Latvijas Republikā pirms regulas ieviešanas un izmaiņas datu aizsardzībā kopš tās stāšanas spēkā.

Trešajā daļā tiek sniegti argumenti tam, kāpēc regula ir nepieciešama IT uzņēmumā un ar ko tās pielietojums šādā uzņēmumā atšķiras no pielietojuma vienkāršā komercuzņēmumā.

Ceturtajā daļā tiek analizēta situācija starptautiskā IT uzņēmumā un tiek salīdzināts, kas mainījies gada laikā kopš regulas ieviešanas.

Piektā un sestā daļa satur autores praktisko darbu – regulas pielietojuma vadlīnijas IT uzņēmumā un rīku ieteikumus datu kontrolierim. Vēl autore veica uzņēmuma izmantotās sistēmas analīzi, testēšanu un novērtēšanu.

Pēdējā daļā tiek apkopoti darba gaitā sasniegtie rezultāti un secinājumi.

1. VISPĀRĪGĀ DATU AIZSARDZĪBAS REGULA

2018. gadā spēkā stājās jaunā Eiropas Savienības Vispārīgā datu aizsardzības regula, kā rezultātā uzņēmumiem radās jautājumi un neskaidrības par tās pielietojumu. Šajā nodaļā tiek aprakstīta regulas ieviešanas nepieciešamība un regulas aizsargājamie dati.

1.1. Vispārīgās datu aizsardzības regulas ieviešanas nepieciešamība

Dzīvojot straujajā tehnoloģiju attīstības laikmetā, kļūst skaidrs, ka datu glabāšana papīra formātā ir ļoti neērta un izšķērdīga attiecībā pret dabas resursiem. Mūsdienu cilvēki, neaizdomājoties par sekām, arvien biežāk tīmeklī atstāj savus datus, piemēram, lietojot sociālos tīklus vai meklējot nepieciešamo informāciju. Dažādas organizācijas šos datus labprāt izmanto savu mērķu sasniegšanai, pārsvarā mārketingam. 2019. gada sākuma statistika vēsta, ka gandrīz 4,4 miljardi cilvēku bija aktīvi tīmekļa lietotāji un 3,5 miljardi bija sociālo mediju lietotāji. [1]

Personas dati tiek apstrādāti, glabāti un pārsūtīti ne tikai ārējā tīmeklī, bet arī dažādu uzņēmumu iekšējā sistēmā. Tās var būt gan valsts iestādes, gan privātie uzņēmumi. Dati var piederēt gan klientiem, gan iekšējiem darbiniekiem. Sakarā ar datu apgrozības un glabāšanas pieaugumu, kā arī ērtāku izmantošanu iestādes un uzņēmumi sāka atteikties no arhīviem un pierakstiem papīra formātā. Mūsdienās datu glabāšanu veic uzņēmuma serverī vai mākonī.

Ar laiku un pieredzi kļuva skaidrs, ka datu drošības regulējumam ir jāmainās, lai atbilstu mūsdienu metodēm. Iepriekšējā 1995. gada Eiropas Savienības datu aizsardzības direktīva "Par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti" jau bija novecojusi, tāpēc 2016. gadā stājās spēkā Eiropas Savienības Vispārīgā datu aizsardzības regula, savukārt 2018. gada 25. maijā tā kļuva piemērojama visās ES dalībvalstīs. Atšķirībā no direktīvas regula ir saistoša visām ES dalībvalstīm, tāpēc radās nepieciešamība izveidot vienādu datu aizsardzības regulējumu visām dalībvalstīm, kas iepriekš katrai no tām varēja atšķirties.

Jāņem vērā, ka regulas ieviešana skāra ne tikai ES dalībvalstu, bet arī citu valstu uzņēmumus, kam regula būs jāievēro tajos gadījumos, ja tie saglabā vai apstrādā ES dalībvalstu pilsoņu vai nepilsoņu datus. VDAR ieviešanas sekas izpaužas arī tā, ka daži uzņēmumi atsakās apkalpot ES pilsoņus. Piemēram, apmeklējot tīmekļa portālu *New York Daily News*, uzreiz var redzēt brīdinājumu par to, ka tīmekļa vietne pašlaik nav pieejama lielākajā daļā Eiropas valstu.

[2] Tā, piemēram, arī daži tīmekļa videospēļu uzņēmumi bloķē ES pilsoņu piekļuvi vecākiem produktiem, nevis mēģina tos atjaunināt, lai spēles atbilstu VDAR prasībām. [3]

1.2. Vispārīgās datu aizsardzības regulas aizsargājamie dati

Pateicoties regulai, šobrīd katrai fiziskai personai ir tiesības zināt, kā tiek apstrādāti tās dati, kādi tie ir, kāpēc tie tiek izmantoti un kur tie tiek apstrādāti un glabāti. Tas sniedz personai iespēju gan piekrist, gan atteikties no savu datu izmantošanas. Jo sevišķi tas var novērst personas datu ļaunprātīgu izmantošanu.

Personas dati ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu. [4] VDAR paplašina definīciju un nosaka, ka identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem [5].

Personu identificēšana var notikt tieši vai netieši. Tiešā identificēšana satur informāciju jeb identifikatoru, kas uzreiz saistās ar konkrētu personu, piemēram, vārds un uzvārds. Netiešajai personas identificēšanai ir nepieciešami papildu rīki un darbības. Piemēram, ja personu mēģina identificēt pēc IP numura.

Par personas datiem var uzskatīt šādus datus:

1. vārds un uzvārds;
2. darbavieta;
3. ieņemamais amats;
4. mājas adrese;
5. e-pasta adrese;
6. personas kods, personu apliecinošu dokumentu numurs;
7. atrašanās vietas dati;
8. interneta protokola (IP) adrese;
9. sīkdatnes identifikācijas numurs;
10. ārstniecības iestādē glabātie dati par pacientu u. tml. [6]

Turpretī par personas datiem nav uzskatāmi tādi dati, kuri var atteikties uz vairākām personām, jo tādā gadījumā konkrēta persona nevar tikt identificēta. Personas dati neattiecas uz mirušām personām, kamēr vien pēc mirušo personu datiem nevar identificēt dzīvu personu.

Arī informācija par juridisku personu netiek uzskatīta par personas datiem. Regula neaizsargā anonimizētus datus. No tā var secināt, ka šie dati var kļūt par personas datiem tikai tad, ja kontekstā tie ir saistīti ar konkrētu personu.

Ir svarīgi izdalīt atsevišķi minētu personas datu apakškategoriju – sensītīvie dati. Sensitīvie personas dati – personas dati, kas norāda personas rasi, etnisko izcelsmi (tautību), reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi. [7] Sensitīvus datus var apstrādāt tikai īpašos gadījumos, kas ir noteikti regulas 9. panta 2. punktā.

Mūsdienās personas datiem ir liela vērtība, un šobrīd piekļuve tiem ir vieglāka. Pēc personas datiem var viegli atrast cilvēku, saprast viņa paradumus, dzīvi, ģimenes stāvokli un intereses. Tāpēc tiem ir jābūt īpaši pasargātiem un izmantotiem tikai ar datu īpašnieka piekrišanu un uzraudzību. Tādēļ, pēc autores domām, Vispārīgās datu aizsardzības regulas nosacījumi par datu izmantošanu ļautu cilvēkiem justies informētiem un pasargātiem.

2. VDAR PIELIETOJUMS LATVIJAS REPUBLIKĀ

Latvija pievienojās Eiropas Savienībai 2004. gada 1. maijā, un tā ir Eiropas Savienības dalībvalsts. Sakarā ar to VDAR ieviešana bija obligāts pasākums, kas skar arī Latvijas tā laika likumdošanu.

2.1. Datu aizsardzības regulējums pirms regulas stāšanās spēkā

Personas datu drošība ir ļoti svarīga, jo tā ir saistīta ar personas privāto dzīvi. Cilvēki lielākoties nevēlas, lai viņu privātā dzīve tiktu jebkādā veida aizskarta. Latvijas Republikas Satversmē un starptautiskajos normatīvajos aktos ir noteikts, ka katram no mums ir paredzētas tiesības uz privāto dzīvi – tiesības domāt to, ko gribam, darīt to, ko gribam, un būt tādiem, kādi esam. [5] No tā izriet, ka jebkura mūsu datu analīze un novērtējums ir tieša iejaukšanās mūsu privātajā dzīvē.

Tā kā Latvijas Republika kopš 2004. gada ir ES dalībvalsts, tai ir piemērojama Eiropas Savienības pamattiesību harta, kas stājās spēkā 2012. gadā. Šī harta ir viens no primārajiem tiesību aktiem, kas nosaka ES darbību.

Hartas 8. pants apraksta Personas datu aizsardzības principu:

"1. Ikvienai personai ir tiesības uz savu personas datu aizsardzību.

2. Šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.

3. Atbilstību šiem noteikumiem kontrolē neatkarīga iestāde." [9]

Iepriekš pastāvēja divas ES direktīvas, kas tika saistītas ar datu aizsardzību pirms VDAR ieviešanas. Svarīgi pieminēt, ka direktīva ir sekundārs tiesību akts un tā nav tieši piemērojama ES dalībvalstīm, tomēr tās noteikumi var būt ieviesti dalībvalstu nacionālajos likumos. Pirmā direktīva ir Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. Šī direktīva zaudēja savu spēku, kad stājās spēkā VDAR. Otrā direktīva ir Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK11 par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju). Šī direktīva attiecas uz datu aizsardzību digitālajā vidē. Šī direktīva ir spēkā joprojām.

No 2000. gada Latvijā stājās spēkā Fizisko personu datu aizsardzības likums. Tā mērķis bija aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību attiecībā uz fiziskās personas datu apstrādi [10]. Likumā ir minēts, ka tajā ir iekļautas tiesību normas, kas izriet no Eiropas Parlamenta un Padomes 1995. gada 24. oktobra direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. Tas nozīmē, ka Latvijas Republika pielietoja direktīvu normas savā likumā. Šis likums zaudēja spēku 2018. gada 5. jūlijā līdz ar jaunā Fizisko personu datu apstrādes likuma ieviešanu.

Ar datu aizsardzības regulējumu no 2001. gada Latvijā nodarbojas Datu valsts inspekcija, kas atrodas Tieslietu ministrijas pārraudzībā. Tā darbojas, pamatojoties uz 2013. gada Ministru kabineta noteikumiem Nr. 1415 "Datu valsts inspekcijas nolikums" un Fizisko personu datu aizsardzības likumu. Ir jāpiemin, ka Eiropas Savienības pamattiesību harta un direktīva noteica, ka iestādei, kas nodarbojas ar datu aizsardzību, ir jābūt neatkarīgai, bet Datu valsts inspekcijas darbība ir atkarīga no Tieslietu ministrijas.

Administratīvajā pārkāpumu kodeksā ir paredzēti sodi par nelikumīgām darbībām saistībā ar personas datu aizsardzību. Tie bija aprakstīti kodeksa 204.^{7}, 204.^{8}, 204.^{9} , 204.^{10} pantā. Atbildīgā iestāde, kas izskata šos pārkāpumus, ir Datu valsts inspekcija. Datu valsts inspekcijas vārdā izskatīt administratīvo pārkāpumu lietas un uzlikt administratīvo sodu ir tiesīgs Datu valsts inspekcijas direktors un viņa pilnvaroti darbinieki [11].

Ir skaidrs, ka personas datu aizsardzība Latvijā notika vēl pirms valsts pievienojās Eiropas Savienībai, jo Fizisko personu datu aizsardzības likums un Datu valsts inspekcija eksistēja jau kopš 2000. un 2001. gada. Vēlāk valsts likums tika grozīts, un tad tas jau saturēja ES direktīvu normas. Tomēr šis likums zaudēja spēku un arī citi normatīvie akti tika grozīti, kad stājās spēkā jaunā VDAR.

2.2. Izmaiņas datu aizsardzībā pēc VDAR stāšanās spēkā

Pēc regulas stāšanas spēkā Latvijas Republikas likumdošanā būtu jānotiek vairākiem grozījumiem tiesību aktos, kas ir saistīti ar datu aizsardzību. Svarīgi pieminēt, ka šīs izmaiņas notika ne vien valstiskā līmenī, bet arī dažādu organizāciju līmenī, kurām bija jāmaina iekšējie noteikumi. Šajā nodaļā tiks izskatītas izmaiņas, kurām būtu jāparādās pēc regulas nosacījumu ieviešanas valstī, un tas, kā šīs izmaiņas tika realizētas.

2.2.1. Jaunās atbildības un tiesības

Tā kā regula ir primārs tiesību akts, tā ir tieši piemērojama visās Eiropas Savienības dalībvalstīs, kas nozīmē, ka tagad visiem nacionālajiem tiesību aktiem ir jāatbilst regulas nosacījumiem. Sakarā ar to 5. jūlijā Latvijā stājās spēkā jauns Fizisko personu datu apstrādes likums, kas aizvietos veco Fizisko personu datu aizsardzības likumu. Eksperti uzskata, ka kopumā jaunā likuma ieviešana nemaina līdzšinējos personas datu apstrādes principus, kas bija noteikti Fizisko personu datu aizsardzības likumā.[12]

Ar regulas ieviešanu fiziskai vai juridiskai personai, kas nodarbojas ar datu apstrādi komerciāliem vai profesionāliem nolūkiem, palielinājās atbildība un pienākums nodrošināt, lai personas datu apstrāde ir likumīga, godprātīga un pārredzama.[12] Tas arī nozīmē, ka personai, kuras dati tiek apstrādāti, paplašinājās tiesības kontrolēt savu datu izmantošanu.

Tiesību paplašinājums nozīmē to, ka persona var būt informēta, kā un kādam nolūkam tās dati tiek izmantoti. Šādas tiesības izpaužas kā tiesības uz datu pārnesamību; tiesības tikt informētam; tiesības iebilst; tiesības tikt aizmirstam u.c. Autore uzskata, ka šī darba ietvaros ir nepieciešams paskaidrot katru no tiesībām.

Tiesības uz datu pārnesamību nozīmē to, ka personai, kas ir datu subjekts, ir iespēja saņemt savus personas datus, ko tā ir sniegusi pārzinim. Šiem datiem ir jābūt strukturētā, vispārpieņemtā un mašīnsalasāmā formātā. Tāpat persona var pārsūtīt tos pašus datus citam pārzinim. Šīs tiesības ir vērstas uz datu subjektu iespējām viegli pārvietot, kopēt vai pārsūtīt personas datus no vienas IT vides uz citu [13].

Tiesības tikt informētam nozīmē, ka datu pārzinim ir jāinformē subjekts par to, kādā veidā tā personas dati tiks izmantoti un kādā nolūkā. Datu pārzinim tagad ir nepieciešams saņemt subjekta piekrišanu. Svarīgi pieminēt, ka piekrišana nav mūžīga un personai ir tiesības atsaukt savu piekrišanu un aizliegt datu apstrādi. Šis aizliegums neattiecas uz datu apstrādi, kas tika veikta pirms atsaukuma, pamatojoties uz iepriekšējo piekrišanu. Tiesības sniedz datu subjektam iespēju iebilst pret savu datu izmantošanu.

Pēc autores domām, svarīgākās tiesības ir tiesības tikt aizmirstam. Tās nozīmē to, ka subjektam ir iespēja pieprasīt, lai tiktu pārtraukta tā datu apstrāde, un izteikt vēlēšanos, lai datus dzēš no visiem serveriem un reģistriem. Tomēr, kā minēja Tieslietu ministrijas Nozaru politikas departamenta direktore O. Zeile, ir jāvērtē, ar kādu mērķi un uz kāda pamata šī datu apstrāde ir notikusi. Ja tā notikusi saskaņā ar noteiktiem likumiem, nav pieļaujams, ka visi personas dati tiek

dzēsti. Piemēram, Valsts sociālās apdrošināšanas aģentūrai nevarēs pieprasīt, lai dzēš visus personas datus, taču to varēs pieprasīt, piemēram, sociālajam tīklam [14].

Svarīgs jauninājums ir vispārējs paziņošanas pienākums par personas datu aizsardzības pārkāpumu. Saskaņā ar VDAR 33. panta 1. punktu personas datu aizsardzības pārkāpuma gadījumā pārzinis bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, paziņo par personas datu aizsardzības pārkāpumu uzraudzības iestādei, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām [5]. Ja paziņojums tika kavēts un tika atklāts pēc 72 stundām, tam jāpievieno arī kavēšanas iemesls. Ja pārkāpums rada lielu risku iesaistītajiem datu subjektiem, tad jāinformē arī šīs personas. Tas nav jādara tikai tad, ja risks tika veiksmīgi novērsts. Piemēru saistībā ar IT joma iespējamo pārkāpumu sniedz Eiropas Komisija: "Kāds mākoņdatošanas pakalpojumu sniedzējs nozaudē vairākus cietos diskus, kas satur personas datus, kuri pieder vairākiem klientiem. Tam par šo incidentu ir jāinformē savi klienti, tiklīdz tas ir uzzinājis par pārkāpumu. Atkarībā no tā, kāda veida datus apstrādājis datu apstrādātājs, klientiem ir jāinformē arī datu aizsardzības iestāde un attiecīgās fiziskās personas."[15]

Līdz ar regulas ieviešanu uzņēmumiem un iestādēm rodas uzdevumi saistībā ar pārskatatbildību. To var paskaidrot tā, ka uzņēmumam jāspēj pieradīt, ka personas datu apstrāde atbilst regulas prasībām. Pat ja uzņēmumā nebija pamanīts datu aizsardzības pārkāpums, tam tāpat ir jāspēj pierādīt, ka regula tiek ievērota. No tā izriet, ka ir nepieciešams pieņemt iekšējos noteikumus, politiku par personas datu aizsardzību, apmācīt savus darbiniekus un nozīmēt atbildīgos.

2.2.2. Par datu aizsardzību atbildīgās personas

Pēc regulas nosacījumiem tagad iestādē vai uzņēmumā ir jābūt atbildīgajai personai, pārzinim vai apstrādātājam, kas nodarbosies ar datu uzraudzību vai apstrādātajiem datiem. Saskaņā ar VDAR 11. punktu, lai personas datu aizsardzība visā Eiropas Savienībā būtu efektīva, nepieciešams piešķirt arī atbilstošas pilnvaras uzraudzīt un nodrošināt personas datu aizsardzības noteikumu ievērošanu dalībvalstīs [5].

Pirms regulas ieviešanas pārzinim, kas vēlējas sākt jebkādu datu apstrādi Latvijas Republikā, bija jāreģistrējas Datu valsts inspekcijā. Regula atceļ šādu reģistrāciju, un pārzinim vairs nebūs jāvēršas Datu valsts inspekcijā. Bet tas nenozīmē, ka pārziņa darbības un uzdevumi kļuvuši vieglāki. Pārzinim radās pienākums gan ieviest personas datu reģistru, kurā ir noteikti datu

apstrādes mērķi, datu glabāšanas termiņi, dzēšanas nosacījumi, gan arī sniegt personai skaidru un saprotamu informāciju par to, kāpēc pārzinim ir nepieciešami personas dati un kas ar tiem tiek darīts [8].

Regulā tiek atrunāta datu aizsardzības speciālista institūta izveide. VDAR 37. pantā ir noteikti gadījumi, kad organizācijai ir jāizvēlas speciālists. Tie ir, ja datu apstrādi veic valsts iestāde vai struktūra, ja organizācija apstrādā sensitīvus datus un datus par sodāmību un noziedzīgiem nodarījumiem vai arī tad, ja nepieciešama sistemātiska un regulāra datu subjektu novērošana. Šie specialisti darbojas kā iekšējais uzraugs iestādē vai organizācijā. Tie informē un konsultē pārzini par datu aizsardzības prasībām, uzrauga regulas prasību ievērošanu, sniedz padomus, sadarbojas ar uzraudzības iestādi un ir kontaktpersona jautājumos, kas saistīti ar apstrādi, it īpaši datu subjektam īstenojot savas tiesības [16]. Pēc autores domām, iepriekšminēto speciālistu var salīdzināt ar iekšējo auditoru tāpēc, ka tiem ir līdzīgs neatkarības un neitralitātes statuss. Speciālistam, vērtējot pārziņa darbu, ir jābūt neatkarīgam savos lēmumos un savā darbībā, lai gan viņu ir nodarbinājusi konkrēta iestāde vai organizācija.

2.2.3. Sodi par pārkāpumiem

VDAR iekļauj sevī arī jaunus sodus, kuru summu apjoms jau no paša sākuma pievērsa sev daudz uzmanības un tika plaši apspriesta. Izpētot regulu, kļūst skaidrs, ka administratīvā soda apjoms pieaug līdz 20 miljoniem eiro vai līdz 4% no uzņēmuma kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma.. Lai arī šīs summas šķiet biedējošas, tomēr piemērotais sods būs atkarīgs no pārkāpuma smaguma un citiem faktoriem. Dažos gadījumos tiek paredzēts vienkāršs brīdinājums.

Datu valsts inspekcija savos iekšējos dokumentos min, ka par regulas noteikumu pārkāpšanu jāpiemēro "līdzvērtīgas sankcijas", savukārt administratīviem naudas sodiem ir jābūt "iedarbīgiem, samērīgiem un atturošiem" [17] .Tas nozīmē, ka visiem sodiem par datu aizsardzības pārkāpumiem ir jābūt aprēķinātiem, ņemot vērā nodarīto kaitējumu un tā sekas.

VDAR 83. panta 4., 5. un 6. punktā ir uzskaitīti pārkāpumi un administratīvie sodi, kurus piemēro, ja pārziņa vai apstrādātāja darbībā ir konstatēti pārkāpumi. 83. panta 7. punktā ir norādīts, ka dalībvalsts var izstrādāt savus ieteikumus par to, līdz kādam apjomam administratīvos naudas sodus var piemērot publiskām iestādēm un organizācijām.

Pēc regulas ieviešanas jauninājumi ir pamanāmi organizatoriskajos jautājumos, kas saistīti ar jaunu amatu izveidi, pārkāpuma paziņojumu un datu subjekta informēšanu par tā datu izmantošanu.

Tika paplašinātas subjekta tiesības uz saviem datiem un pārziņa atbildība un uzdevumi saistībā ar šo datu apstrādi. Vairāki autori uzsver, ka regulas ieviešana nav revolūcija, bet evolūcija, un autore piekrīt šīm uzskatam. Mūsdienu tiesību sistēmai un likumdošanai ir jāatbilst jaunajam tehnoloģiju laikmetam. Sistēmai jābūt caurspīdīgai attiecībā pret datu subjektiem, it īpaši digitālajā vidē, kurā iepriekš pastāvēja neskaidrības par lietotāju datu izmantošanu un apstrādi, un tajā laikā personas dati varēja tikt viegli izmantoti ļaunprātīgos nolūkos.

3. REGULAS NEPIECIEŠAMĪBA IT UZŅEMUMĀ

Eiropas Savienības Vispārīgās datu aizsardzības regulas nosacījumi attiecas uz jebkura tipa uzņēmumu, kas jebkādā veidā nodarbojas ar personas datu glabāšanu un apstrādi neatkarīgi no tā darbības jomas. Tie var būt uzņēmuma klientu dati, kā arī darbinieku dati. Pat ja klienti vai darbinieki var būt juridiskas personas, tomēr pārsvarā dati pieder juridisko personu pārstāvjiem, kas ir fiziskas personas.

Pēc autores domām, regulas ieviešanu IT uzņēmumā var apskatīt atsevišķi, jo tas bieži nodarbojas ar sistēmu izstrādi, kas realizēs datu glabāšanu un apstrādi mūsdienīgajā digitālajā veidā. Tādam uzņēmumam vēl nopietnāk ir jāpievērš uzmanība VDAR nosacījumiem. Piemēram, izstrādājot sistēmas, lietotājam ir jādod iespēja piekrist savu datu apstrādei, kā arī pēc tam nodrošināt administratoram iespēju pēc lietotāja pieprasījuma viegli dzēst šos datus. Tāpat būtu pareizi nodrošināt datu glabāšanu, šifrējot šos datus, jo vienmēr jāapzinās, ka pastāv datu noplūdes iespēja.

No iepriekšminētā izriet, ka regulas prasības tieši ietekmē IT uzņēmuma darbību, jo parasti tā darbība balstās uz projektiem, ko uzņēmums realizē. Datu bāžu un e-komercijas projekti ir tikai viens no piemēriem, kas saistīts ar lieliem personas datu apjomiem. Ir vērts minēt arī vel nopietnāku IT projektu jeb sociālo tīklu izveidi. Tas ir nopietns tāpēc, ka sociālajos tīklos var tikt glabāti personas sensitīvie dati.

Pēc autores domām, uzņēmumam ir jāapmāca un jāinformē savi darbinieki par VDAR un tās prasībām, īpaši tos, kas nodarbojas ar sistēmu izstrādi un testēšanu. Tas ir svarīgi, jo darbinieki izstrādes laikā uzreiz var piedāvāt klientam un integrēt izstrādājamajā sistēmā dažas metodes, kas palīdzēs apstrādāt lietotāju datus, ievērojot VDAR prasības. Tas paaugstinās klienta uzticību uzņēmumam.

Autore ir apkopojusi viedokļus par to, kam izstrādājam ir jāpievērš uzmanība, izstrādājot sistēmu. Vispirms ir svarīgi atcerēties, ka sistēmas gala lietotājam ir plašs tiesību klāsts:

1. Tiesības ierobežot apstrādi. Datus joprojām var glabāt sistēmā, bet ir jāierobežo to tālāka izmantošana. Piemēram, var izveidot jaunu tabulu datu bāzē, kur tiks glabāti dati, kurus jāierobežo.

2. Tiesības uz datu pārnesamību. Sistēmas administratoram vai lietotajam ir jābūt iespējai saņemt subjekta pieprasītos datus mašīnlasāmā formātā un pārsūtīt to citam pārzinim. Lietotājam ir jādod iespēja komunicēt ar personu, kas varēs pārsūtīt šos datus, vai arī jābūt pieejamai funkcijai, kas atļaus to izdarīt viņam pašam.

3. Tiesības labot datus. Cilvēki bieži ar to saskaras, rediģējot savu profilu sociālajos tīklos vai mainot e-pastu vai paroli citās sistēmās. Lietotājam ir jābūt iespējai realizēt šīs tiesības bez kavēšanas, nevis gaidīt ilgu atbildi no administratora puses, kamēr viņa dati tiks izmainīti.

4. Tiesības datu piekļuvei. Lietotājam var dod iespēju redzēt visus datus, kas par viņu tiek uzglabāti. Vai arī viņam jāsniedz informācija pirms viņa datu nodošanas sistēmā par to, kādi dati tiks glabāti un izmantoti, lai viņš var sniegt savu piekrišanu.

5. Tiesības būt informētam. Šīs tiesības izpaužas kā informācijas caurspīdīgums. Datu subjektam ir jābūt skaidri saprotams, kā tiek izmantoti tā dati. Visai informācijai, ko sistēma sniegs par datu izmantošanu un glabāšanu, ir jābūt viegli lasāmai un saprotamai. Iepriekš ļoti daudzas sistēmas saturēja garus noteikumus, ko lielākā daļa lietotāju nemaz nelasīja. Tagad lietotāji to atcēla. Nedrīkst aizmirst, ka lietotājam var sniegt iespēju izvelēties, kādos vēl nolūkos viņa dati var tikt izmantoti. Tas cels arī lietotāja uzticību produktam. Piemēram, viņš var piekrist savu datu izmantošanai reģistrācijai, bet neparakstīties uz sistēmas jaunumu sūtīšanu.

6. Tiesības būt aizmistam. Sistēmas administratoram ir jābūt iespējai vienkāršā veidā izdzēst datus pēc datu subjekta pieprasījuma, vai arī tam jānotiek pēc tam, kad lietotājs dzēš savu profilu.

Uzņēmumam ir pienākums informēt trešās personas, kuras arī piedalījušās datu subjekta datu apstrādē, par izmaiņām subjekta datos vai par datu dzēšanu. To var realizēt, vienkārši nosūtot paziņojumu ar jaunajiem datiem vai brīdinājumu par datu dzēšanu uz trešās personas e-pastu manuāli vai arī automātiski.

Regula pievērš uzmanību arī datu subjekta vecumam. Ja lietotājs nav sasniedzis 16 gadu vecumu, datu glabāšanai un apstrādei ir nepieciešama viņa vecāku piekrišana. Tad sistēmā ir jāveic personas dzimšanas gada vai vecuma pārbaude. Ja, persona sniedz nepatiesu informāciju par savu vecumu, datu apstrādātājs nenes par to atbildību.

Sistēmā ir jāglabā tikai svarīgi un tiešām nepieciešami dati. Tāpēc jau sākotnēji ir jāizvērtē, kādi dati ir nepieciešami. Tāpat ir svarīgi izstrādes laikā parūpēties par personas datu glabāšanas termiņu un nepieciešamību. Ir jāpievērš uzmanība datu glabāšanas termiņiem. Var rasties šāda situācija, kad sistēma dod iespēju veikt pasūtījumus nereģistrētiem lietotājiem. Ir jāsazinās ar klientu, lai noskaidrotu, cik ilgai datu uzglabāšanai viņš piekrīt – pēc pasūtījuma piegādes vai pēc produkta garantijas laika. Kad nosacījumi tiks izpildīti, klienta dati tiks izdzēsti no sistēmas, vai anonimitāte tiks garantēta tādā veidā, kāds ir nepieciešams uzņēmumam.

Jebkuram uzņēmumam ir jābūt iespējai nodrošināt saviem darbiniekiem un klientiem drošu datu apstrādi un glabāšanu. Datus, kas glabājas digitalizētā veidā, uzņēmumam ir jāmēģina šifrēt, anonimizēt vai pseidonimizēt. Uzņēmumam jānolemj, kuri dati ir svarīgi glabāšanai. To svarīgi nolemt jau pašā sākumā, jo profilakse ir vieglāka nekā ārstēšana. Tādā veidā tiks minimizēts uzglabāto datu apjoms. IT uzņēmumam ir jāpievērš īpaša uzmanība savu darbinieku apmācībām, jo tie var būt saistīt ar tādu sistēmu izveidi, kurām jāatbilst VDAR, tādēļ viņu kompetence šādos jautājumos tikai cels klienta uzticības līmeni.

4. SITUĀCIJA STARPTAUTISKĀ IT UZŅĒMUMĀ

Pirms šī bakalaura darba izstrādes uzsākšanas autore pētīja situāciju ar VDAR ieviešanu starptautiskā uzņēmumā 2018. gadā maijā pirms regulas stāšanās spēkā. Šajā nodaļā autore apskatīs situāciju, kas bija iepriekš, un salīdzinās to ar situāciju, kas ir šobrīd, jo kopš regulas ieviešanas jau pagājis gandrīz pilns gads.

4.1. Iepriekšējā situācija uzņēmumā

2018. gadā autorei radās iespēja novērot, kā VDAR tiek ieviesta starptautiskā IT uzņēmumā. IT uzņēmums pārsvarā nodarbojas ar e-komercijas sistēmu ražošanu, tātad arī sistēmas, ko uzņēmums izstrādā, ir pārsvarā saistītas ar personas datu glabāšanu. Uzņēmums sadarbojas ar klientiem no visas pasaules. Tā kā tas ir starptautisks uzņēmums, tā filiāles atrodas dažādās valstīs un dažādos kontinentos: Eiropā, Amerikas Savienotajās Valstīs, Dienvidāzijas reģionā un Austrālijā. No tā izriet, ka gan uzņēmuma darbinieki, gan klienti ir no Eiropas Savienības, tātad uz viņiem attiecas VDAR.

Tobrīd pēc mutiskas aptaujas kļuva skaidrs, ka tikai uzņēmuma vadītajiem bija zināms par VDAR ieviešanu un tās nosacījumiem, jo tie piedalījās dažādos semināros, tomēr neviens tajā necentās iedziļināties. Savukārt darbinieku zināšanas par regulu bija vispārīgas, nevis konkrētas attiecībā uz savām tiesībām. Pēc autores domām, toreiz uzņēmumā bija jārīko semināri par regulas ieviešanu, lai varētu apmācīt visus darbiniekus.

Autore intervēja personu, kura ir atbildīga par regulas pielietojumu uzņēmumā. Vispirms autorei bija nepieciešams uzzināt, kas uzņēmumā nodarbojas ar datu aizsardzību, jo tas ir starptautisks. Pēc intervijas kļuva skaidrs, ka uzņēmuma datu pārzinis atrodas Vācijā.

Nākamais jautājums bija par iekšējiem noteikumiem, kas bija jāizstrādā reizē ar regulas ieviešanu. Toreiz kļuva skaidrs, ka noteikumi jau pastāv, bet joprojām tiek papildināti un grozīti, jo, pēc intervējamās personas teiktā, regulas nosacījumus nav tik vienkārši apvienot ar darba procesu. Toreiz noteikumi bija pieejami tikai vācu valodā, tāpēc ne visi darbinieki varēja ar tiem iepazīties.

Runājot par datu apstrādi un glabāšanu, autore secināja, ka sensitīvie dati netiek apstrādāti. Intervējamais pauda, ka datu glabāšana un apstrāde notiek, izmantojot C4C sistēmu un Microsoft sistēmas. Visi dati par darbiniekiem, projektiem un klientiem tika glabāti serverī un pasargāti ar parolēm. Tomēr pastāvēja datu šifrēšanas nepilnības, īpaši saistībā ar projektu pierakstiem.

Bija interesanti uzzināt, ko eksperts domā par datu aizsardzības atšķirībām katrā no valstīm ārpus Eiropas Savienības, kur atrodas uzņēmuma filiāles. Tika ievēroti arī katras valsts nacionālie likumi un noteikumi. Bija skaidrs, ka katrā valstī pastāv savs regulējums. Kā piemēru eksperts minēja 2016. gada "ES un ASV privātuma aizsardzības" [18] nolīgumu. Nolīgums nodrošina:

- stingras datu aizsardzības prasības uzņēmumiem, kas saņem personas datus no ES;
- drošības garantijas ASV valdības piekļuvei datiem;
- efektīvu aizsardzību un atlīdzību personām;
- ES un ASV ikgadēju kopīgu pārskatu, lai uzraudzītu pareizu vienošanās piemērošanu. [18]

Toreiz intervējamais sacīja, ka ir doma nosūtīt katram darbiniekam līgumu par viņa datu izmantošanu elektroniskā veidā, lai viņš tam piekristu.

Autore centās atrast informāciju par savu datu glabāšanu un nodošanu uzņēmumam sava darba līgumā, tomēr līgumā sīkāk tika atrunāti tikai uzņēmuma dati.

Pēc intervijas tapa skaidrs, ka uzņēmums gatavojas jaunās regulas ieviešanai, tomēr tas notiek starp uzņēmuma vadošo amatu pārstāvjiem. Tika pausts, ka uzņēmumā tiks izstrādāti iekšējie noteikumi saistībā ar datu apstrādi, kas atbildīs regulai, un bija plānots paaugstināt datu glabāšanas drošību, izmantojot šifrēšanu.

Autoresprāt, ir pozitīvi, ka uzņēmumam ir izvēlēts pārzinis, kas būs atbildīgs par datu drošību. Autorei tika piedāvāts piedalīties iekšējo noteikumu izstrādē un diskusijā par tiem, kā arī paust savu viedokli par noteikumiem, kad tie būs pieejami angļu valodā.

4.2. Pašreizējā situācija uzņēmumā

Gadu pēc VDAR stāšanās spēkā un uzņēmuma sagatavošanas tai autore nolēma izpētīt un salīdzināt, kādas izmaiņas notikušas uzņēmumā, kādi noteikumi tika pieņemti, kā šobrīd notiek datu aizsardzība, glabāšana un šifrēšana un kā notika vai notiks darbinieku apmācības. Pēc autores domām, ir svarīgi uzzināt arī to, vai tiek pielietotas jaunas sistēmas, lai atvieglotu datu drošību, un vai ir izvēlētas datu pārziņa darbības, kā arī vai uzņēmumā jau ir notikuši kādi ar to saistīti pārkāpumi.

Autorei bija iespēja piedalīties intervijā ar personu, kas ir informēta par VDAR pielietojumu uzņēmumā, bet šī persona nebija pats datu kontrolieris. Pirmkārt, autore vēlējas uzzināt, vai ir ieviestas izmaiņas uzņēmuma regulējumā saistībā ar datu drošību. Intervējamais atklāja, ka uzņēmums šogad vairāk pievērsa uzmanību tieši regulas nosacījumu praktiskajam pielietojumam,

tāpēc noteikumi vēl netika iztulkoti. No intervijas kļuva zināms, ka iekšējie noteikumi tika izveidoti, bet tie joprojām ir pieejami tikai vācu valodā. Intervējamais piebilda, ka sakarā ar VDAR ieviešanu uzņēmuma mājaslapā tika izvietoti noteikumi par personas datu izmantošanu. Autore pārbaudīja mājaslapu un atrada šos nosacījumus sadaļā, kur gadījumā, ja trešā persona ātri vēlas pieteikties darbam uzņēmumā, tā uzreiz var sūtīt savus datus un pievienot CV.

Autore uzskata, ka noteikumi ir aprakstīti skaidri un kodolīgi. Tajos tiek minēti nosacījumi par datu izmantošanu, ka tie netiks nodoti trešajām personām un netiks uzglabāti ilgu laiku. Piemēram, ir minēts, ka, nosūtot savus datus saziņai, tie tiks izmantoti tikai tam, lai sazinātos ar pieteicēju, un tad tie tiks dzēsti.

Noteikumos ir minēts, ka personai ir tiesības piekļūt saviem datiem, ko apstrādā uzņēmums. Turklāt personai ir tiesības uz to labošanu, tiesības uz dzēšanu, tiesības uz apstrādes ierobežošanu un tiesības iebilst. Datu subjekts savu piekrišanu var atsaukt jebkurā laikā; jebkurš atsaukums neietekmē apstrādes likumību, pamatojoties uz iepriekšējo piekrišanu, kas tika veikta pirms atsaukšanas. Visas šīs tiesības ir minētas VDAR. Mājaslapā sniegti datu kontroliera dati saziņai.

Noteikumos ir minēts arī par datu izmantošanas kopu ar *Google Analytics*, tīmekļa analīzes pakalpojumu, kas parasti strādā ar *cookies* datnēm. *Cookies* ir pieminēti arī atsevišķi. Šajā nodaļā ir teikts, ka uzņēmuma mājaslapa izmanto tikai vienu *cookie,* un tas sīkdatne ir derīgs tikai septiņas dienas.

Mājaslapas nosacījumos pieminēti arī jaunumi un to pieraksti. Lai pierakstītos jaunumiem, ir nepieciešams nosūtīt savu elektronisko pastu. Nosacījumos ir teikts, ka uzņēmums izmanto tā saukto dubultās izvēles procedūru, lai nodrošinātu, ka jaunumu ziņas tiek nosūtīti konsekventi. Tādējādi potenciālo saņēmēju var iekļaut adresātu sarakstā. Pēc reģistrācijas lietotājs saņem piekrišanas e-pastu, lai apstiprinātu savu vēlmi. Šī adrese tiek aktīvi iekļauta adresātu sarakstā tikai tad, ja reģistrācija ir apstiprināta. Ziņojumu izsūtīšanai tiek izmantota *Newsletter2Go* programmatūra. Vispirms dati tiek pārsūtīti uz *Newsletter2Go,* kam ir aizliegts jebkādā citā veidā apstrādāt vai pārdot personas datus, nevis izsūtīt jaunumus. Šo piekrišanu var atsaukt jebkurā laikā, izmantojot e-pasta adreses abonēšanas atrakstīšanās saiti savā e-pastā.

Nākamais jautājums bija par darbinieku un klientu piekrišanu. Autore atgādināja, ka iepriekš tika paredzēts, ka piekrišanas tiks izveidotas elektroniski. Intervējamais atbildēja, ka tiek plānotas rakstiskas piekrišanas. Šādā veidā tiks grozīti līgumi. Klienti arī tiks informēti, un viņiem tiks sastādītas piekrišanas, tomēr pārsvarā tās būs pieejamas un izsūtītas elektroniski.

Vēlāk tika apspriesta datu glabāšana un to drošība. Intervējamais sacīja, ka tāpat kā iepriekš dati tiek glabāti serverī, kam ir ierobežota pieeja un kam var pieslēgties tikai noteiktas personas.

Autore pieminēja, ka darbiniekiem joprojām netika organizētas apmācības, vismaz vietējā filiālē. Intervējamais atbildēja, ka ir plānots jūnija beigās organizēt semināru visām filiālēm. Semināru rīkos par datu drošību atbildīgā persona, kas noalgota no juridiska uzņēmuma. Intervējamais piekrita arī tam, ka autore uzstāsies ar savu prezentāciju par VDAR vietējā filiālē, kā arī piedāvāja vēlāk apskatīt tapušo prezentāciju un ieteikt, ar ko to var papildināt.

Salīdzinot ar iepriekšējo gadu, uzņēmumā ir novērojama labvēlīga tendence saistībā ar VDAR implementāciju. Tika izveidoti nosacījumi, lai iegūtu trešo personu, kas vēlas pieteikties amatam, piekrišanu. Šie nosacījumi ir caurspīdīgi un kodolīgi. Drīzumā tiek plānotas apmācības, kas palīdzēs arī darbiniekiem uzzināt savas tiesības un to, kā viņi varēs realizēt regulas nosacījumus savos darba uzdevumos. Pēc autores domām, grozījumi līgumā jāizveido pēc apmācībām, lai personām būtu skaidrs, kāpēc šādi grozījumi ir nepieciešami. Uzņēmums uzsāka izmantot sistēmu, kas atvieglos ziņojumu izsūtīšanu klientiem, un tas notiks likumīgi saskaņā ar regulu. Pozitīvākais ir tas, ka uzņēmumā nenotika nekādi ar datu drošības pārkāpumiem saistīti incidenti.

5. REGULAS PIELIETOJUMA VADLĪNIJAS UZŅĒMUMĀ

Lai būtu vieglāk implementēt regulas nosacījumus uzņēmuma darbībās, ir nepieciešams izstrādāt vadlīnijas, kuras datu kontrolierim palīdzēs saprast, vai uzņēmumā viss tiek veikts pareizi, un līdz ar to pieņemt nepieciešamos lēmumus. Iepriekš autore izstrādāja ieteikumus vadlīniju izstrādei, tomēr tie netika izmantoti un vadlīnijas netika izstrādātas, tāpēc autore nolēma izveidot savas vadlīnijas, lai uzlabotu datu aizsardzības situāciju uzņēmumā.

5.1. Datu drošības nodrošinājums

Datu glabāšanai un apstrādei ir jānotiek drošā veidā. Pēc autores domām, to var iedalīt divās apakšnodaļās: organizatoriskā līmenī, kas nozīmē visu iekšējo noteikumu izstrādi un atbildīgo personu iecelšanu, kā arī tehniskā līmenī, kas nozīmē tieši datu apstrādes un glabāšanas procesa drošību, izmantojot mūsdienu tehnoloģijas.

5.1.1. Organizatoriskā līmenī

Viena no svarīgākajām regulas prasībām, kas uzņēmumam ir jāizpilda, ir par datu aizsardzību atbildīgās personas nozīmēšana. Uzņēmumam ir jāizvēlas datu pārzinis. Saskaņā ar VDAR 37. panta otro daļu speciālistam ir jābūt viegli pieejamam katrā filiālē un visām iesaistītajām pusēm. [regula] Tāpat ir svarīgi nozīmēt atbildīgos katrā filiālē. Šīm personām nav jābūt ar datu drošību saistītai izglītībai, taču to uzdevums būs sekot datu aizsardzībai un ziņot pārzinim par pārkāpumiem. Par šādu atbildīgo personu var iecelt speciālistu, kas visvairāk strādā ar datiem – administratoru. Savukārt persona, kas varēs palīdzēt VDAR jautājumos tieši izstrādes posmā, var būt sistēmu izstrādātājs ar vislielāko pieredzi.

Ir jāizveido un jāizdod iekšējie noteikumi saistībā ar datu aizsardzību uzņēmumā. Dokumentos var atsevišķi izdalīt noteikumus par uzņēmuma darbinieku datu glabāšanu un klienta datu glabāšanu. Iekšējiem noteikumiem ir jābūt pieejamiem visiem uzņēmuma darbiniekiem valodā, kurā viņi var tos izlasīt – autores uzņēmuma situācijā – angļu valodā.

Ja darbinieku skaits sasniegs 250 cilvēkus un vairāk, būs jāizstrādā personas datu apstrādes reģistrs, kurā būs fiksētas visas datu apstrādes darbības. Autore uzskata, ka to var izdarīt arī pirms tik liela darbinieku skaita sasniegšanas, jo tas palīdzēs organizēt darbības ar datiem, un reģistrs jebkurā brīdī var atgādināt par darbībām, kas tika veiktas iepriekš. Reģistrs arī palīdz apkopot visu informāciju vienuviet.

5.1.2. Tehniskā līmenī

Ja uzņēmums joprojām glabā savu darbinieku vai klientu informāciju papīra formātā, piemēram, līgumus, šie dokumenti un informācija nedrīkst tikt uzglabāta visiem pieejamā vietā, kā arī atklāti publicēta internetā.

Ir svarīgi personas datus glabāt serverī, kas atrodas aizsargātā vietā, kas nav tik viegli pieejama personām ar ļaunprātīgiem nolūkiem. Tāpat personas datiem, kas tiek glabāti serverī, jābūt šifrētiem.

Regulāri ir jāveic testēšana jeb jāpārbauda, vai piekļūt personas datiem ir vienkārši, jo ar laiku mainās tehnoloģijas un piekļuves iespējas kļūst arvien bīstamākas. Ir jābūt iespējai atgūt datus gadījumā, ja kaut kas notiek ar serveri.

5.2. Datu audits

Ir svarīgi noskaidrot, kādi dati ir uzņēmuma rīcībā, kur tie nonāk un kur tiek glabāti. Ir jāsaprot, kādi subjekta dati ir nepieciešami un no kādiem datiem var atteikties. Jāpievērš uzmanība tam, lai tie nav sensitīvie dati.

Jānolemj, cik ilgi subjekta dati glabāsies, piemēram, gadījumā, ja darbinieks aiziet no darba. Tā kā uzņēmums veic apmācības, tiek ievākti dati par personām, kas tajās piedalās. Taču, ja persona netiek pieņemta darbā, tās dati var tikt uzglabāti kādu laiku vai tiek dzēsti uzreiz.

Īpaša uzmanība jāpievērš situācijai, kad darbinieks aiziet no uzņēmuma. Tas var notikt gan uz draudzīgas nots, gan pretēji. Pēc darbinieka aiziešanas ir jāizdzēš visa informācija no datora, ko viņš izmantoja, kā arī nedrīkst aizmirst par visām attālinātās piekļuves iespējam, ko darbinieks izmantoja, piemēram, projektos. Tāpēc personai, kura nodarbosies ar datu dzēšanu, jāzina par sistēmām, kurām jādzēš piekļuve. Šādos gadījumos vislabāk izmantot tā saucamo "single sign-on" sistēmu, kur lietotājs visur izmanto vienus un tos pašus piekļuves datus, jo vēlāk, piemēram, izdzēšot viņa uzņēmuma nodrošināto e-pastu, viņš vairs nevarēs pieslēgties nekādiem svarīgiem datiem.

5.3. Darbinieku apmācības

Uzņēmuma personāls ir jāapmāca par datu aizsardzību, kā tā realizējas uzņēmumā un kādas ir tā darbinieku tiesības. Savukārt sistēmu izstrādātāji vēl atsevišķi jāinformē par to, kā viņiem būs jāimplementē VDAR nosacījumi sistēmā, lai nosacījumi tiek realizēti pareizi, jo bieži vien pasūtītajam pašam var nebūt skaidrības par regulas pareizu pielietojumu, tāpēc izstrādātājiem jābūt kompetentiem šajā jautājumā, lai celtu klienta uzticību uzņēmumam.

Šajā apakšnodaļā tiek apkopoti svarīgākie jautājumi, kas jāmin darbinieku apmācībās:

1. Datu subjekta tiesības un pieprasījumu apstrāde. Tas nozīmē, ka ir jāpaskaidro darbiniekiem, kādas ir viņu tiesības un kā uzņēmums realizēs viņu pieprasījumus. Uzņēmumam ir jābūt gatavam mēneša laikā sniegt informācijas kopiju par datiem, kas tiek uzglabāti par datu subjektu.

2. Brīdinājums par pikšķerēšanu. Jāatgādina par to, ka darbiniekiem vēlams neizpaust informāciju par klientiem jebkādā veidā.

3. Datu aizsardzības pasākumi. Svarīgi atgādināt darbiniekiem mainīt paroles, dot iespēju instalēt antivīrusu programmas, kā arī runāt par sekām, kas var rasties, atverot aizdomīgas e-pasta vēstules.

Autore sagatavoja prezentāciju, ko izmantoja uzņēmuma Latvijas filiāles darbinieku apmācībām. Šo prezentāciju var izmantot arī citu filiāļu vadītāji savam semināram. Prezentācija tika izvietota uzņēmuma *MS SharePoint* kontā. Prezentācijas slaidus var apskatīt šī darba 1. pielikumā.

5.4. Datu subjekta piekrišanas datu apstrādei

Ir jāsagatavo darbinieku un klientu piekrišanas viņu datu apstrādei un glabāšanai uzņēmuma ietvaros. Saskaņā ar regulas nosacījumiem, ja datu subjektam piekrišana ir jāsniedz pēc elektroniska pieprasījuma, pieprasījumam jābūt skaidram, kodolīgam un tam nav nevajadzīgi jāpārtrauc tā pakalpojuma izmantošana, kuram nepieciešama piekrišana.[5] Tāpēc noteikumiem nevajag būt gariem un jāizvairās no sarežģītas valodas un teikumiem nosacījumu aprakstā.

Pēc autores domām, to ir labāk izdarīt ne tikai elektroniskā veidā, kas, iespējams, ir vieglāk attiecībā pret klientiem, bet arī līgumiskā veidā, lai persona no paša sākuma zina, kādas tai ir tiesības, pienākumi un atbildība. Kas attiecas uz tiesībām, VDAR viss ir skaidri aprakstīts, tomēr personai ir jāatceras, ka tā strādā ar juridisku personu un visas tās darbības darba laikā vai ar

uzņēmuma tehniskajām ierīcēm tiek attiecinātas arī uz uzņēmumu, tāpēc darbībām ir jābūt apdomātam.

Saskaņā ar VDAR 32. pantu klusēšana, iepriekš atzīmēti laukumi vai atturēšanās no darbības nebūtu jāuzskata par piekrišanu. Piekrišanai būtu jāattiecas uz visām apstrādes darbībām, ko veic vienā un tajā pašā nolūkā vai nolūkos. Ja apstrādei ir vairāki nolūki, piekrišana būtu jādod visiem nolūkiem. [5] To iespējams ērti realizēt, sadalot piekrišanas iespējas vairākiem nolūkiem, piemēram, reģistrējoties persona piekrīt nodot savus datus un to atzīmē, bet nepiekrīt saņemt ziņojumus, tāpēc to arī neatzīmē.

Tā kā uzņēmums uztur savu mājaslapu, tas var arī piedāvāt klientiem iespēju pierakstīties uz jaunumu un ziņu saņemšanu. Klientiem ir jābūt iespējai gan piekrist saņemt ziņas, gan iespējai atteikties no ziņu saņemšanas e-pastā, kas var notikt pēc kāda laika. Jāpadomā arī par to, kāda informācija tiek sūtīta klientiem un kāds ir tās noformējums.

5.5. Datu subjekta tiesību atbalsts

Uzņēmumam ir jābūt gatavam profesionāli realizēt datu subjekta tiesības. Pēc VDAR nosacījumiem subjektam ir šādas tiesības:

Datu subjekta piekļuves tiesības;

Tiesības labot;

Tiesības uz dzēšanu;

Tiesības ierobežot apstrādi;

Tiesības uz datu pārnesamību;

Tiesības iebilst;

Šo tiesību realizācijas iespējas var apskatīt regulas 15. , 16., 17., 18., 20. un 21. pantā.

Saskaņā ar regulas nosacījumiem uzņēmumam būtu jāparedz kārtība, kas datu subjektam atvieglotu savu tiesību īstenošanu saskaņā ar šo regulu, tostarp mehānismus, kā pieprasīt un, ja piemērojams, bez maksas saņemt piekļuvi personas datiem, tos labot vai dzēst un īstenot tiesības iebilst. [5] Tā kā uzņēmumam ir daudz darbinieku un klientu, kas atrodas visā pasaulē, un datu pārzinis atrodas tikai vienā vietā, ir skaidrs, ka pieprasījumi tiks veikti elektroniski. Tā kā arī datu apstrāde uzņēmumā notiek pārsvarā elektroniski, ir jānodrošina līdzekļi, ar kuriem pārzinis varēs apskatīt šos pieprasījumus. Tas var būt gan e-pasts, gan rīks iekšējā sistēmā ar pogu par savu datu dzēšanu vai lejupielādēšanu.

5.6. Rīcība datu aizsardzības pārkāpumu gadījumos

Uzņēmumam jābūt gatavam tam, ka var notikt arī datu aizsardzības pārkāpumi. Tas var notikt gan uzņēmuma iekšējā vidē, piemēram, nepareiza darbinieku datu izmantošana vai nelikumīga datu izpaušana bez darbinieka piekrišanas, gan arī neparedzētu apstākļu dēļ, piemēram, var tikt nozagts vai nozaudēts darbinieka dators vai mobilais tālrunis ar klientu datiem. Šajā nodaļā tiek aprakstīts, kam jāpievērš uzmanība un kā pareizi jārīkojas, lai nodrošinātu datu drošību.

Saskaņā ar VDAR 83. pantu, novērtējot datu drošības risku, vērā būtu jāņem riski, ko rada personas datu apstrāde, piemēram, nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem, kas var izraisīt fizisku, materiālu vai nemateriālu kaitējumu. [5] Datu pārzinim ir jāsaprot riski, kas var rasties sakarā ar datu drošības pārkāpumiem. Regulā tiek minētas sekas, kas var rasties līdz ar datu subjekta datu nozaudēšanu. Tie var būt materiāli vai nemateriāli kaitējumi kā, piemēram, iespējas kontrolēt savus personas datus zaudēšana vai to tiesību ierobežošana, diskriminācija, identitātes zādzība vai viltošana, finansiāls zaudējums, neatļauta pseidonimizācijas atcelšana, kaitējums reputācijai, ar dienesta noslēpumu aizsargātu personas datu konfidencialitātes zaudēšana vai jebkāda cita attiecīgajai fiziskajai personai īpaši nelabvēlīga ekonomiskā vai sociālā situācija. [5]

Ja datu subjektam ir radies iespaids, ka viņa dati tiek nelikumīgi izmantoti, viņš var uzrakstīt sūdzību vai pieprasījumu un iesniegt to uzraudzības iestādei. Kontrolierim ir jāzina, ka uz pieprasījumu jāatbild mēneša laikā.

Pārziņa rīcībai pārkāpumu gadījuma ir jābūt šādai: ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, par personas datu aizsardzības pārkāpumu jāpaziņo uzraudzības iestādei, bet, ja to nevar izdarīt 72 stundu laikā, būs nepieciešams pievienot paskaidrojumu. [5] Bet tas nav jādara tādā gadījumā, ja pārzinis varēs pieradīt, ka šis pārkāpums nerada nekādus riskus un tas veiksmīgi tika novērsts.

Ja pārzinis izmanto reģistru, ir svarīgi tajā fiksēt pārkāpumu. Ja reģistra nav, tad var izveidot žurnālu, kurā pārkāpumi tiks ierakstīti. Par pārkāpumu jāatzīmē šāda informācija:

- datums, kurā ir noticis pārkāpums;
- pārkāpuma apraksts, kas satur faktus, kuri apraksta to;
- kā tika paziņots par pārkāpumu;
- dati, kas bija iekļauti pārkāpumā;
- pārkāpuma sekas;

- darbības, kas tika veiktas, lai novērstu nelabvēlīgas sekas datu subjektam.
- nepieciešamība ziņot datu drošības iestādei.

Autoresprāt, izmantojot šādu sadalījumu, var veiksmīgi organizēt uzņēmuma datu drošību risku un pārkāpumu gadījumos.

5.7. Ieteicamais regulas atbalsta rīks

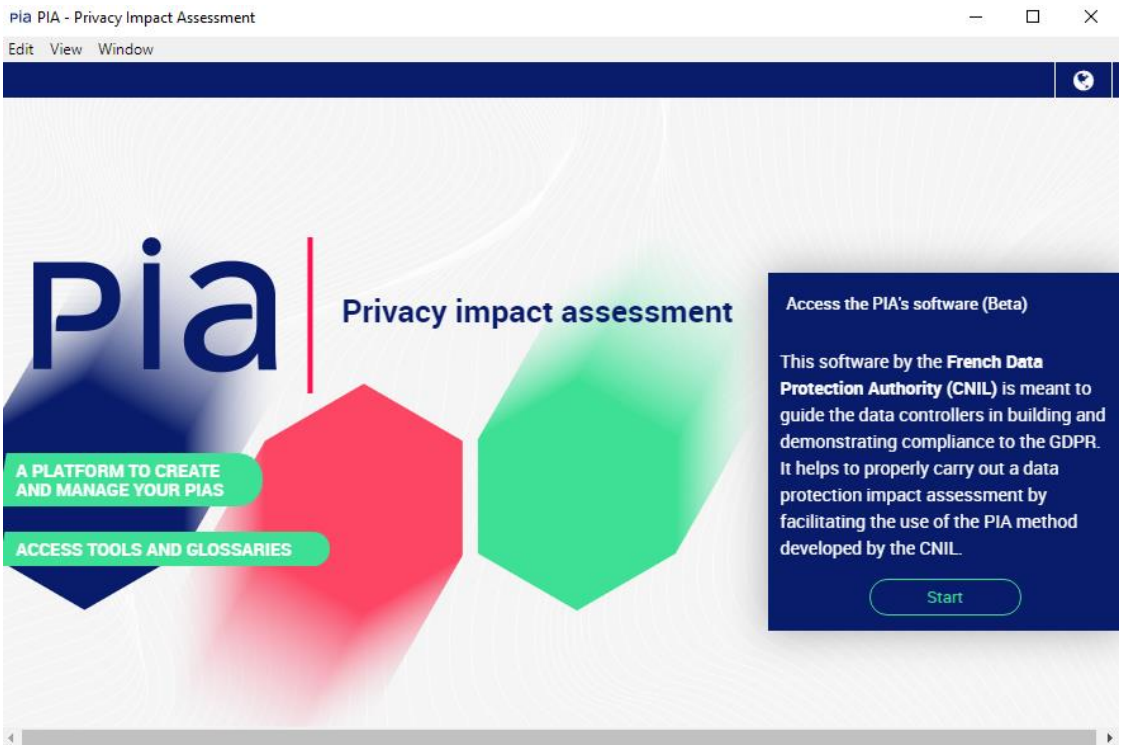
Autore apskatīja rīku, kas varētu palīdzēt organizēt uzņēmuma datu drošību un palīdzēt organizēt datu pārziņa darbu.

Rīks, ar ko autore iepazinās, saucas PIA un angļu valodā nozīmē *privacy impact assessment*, kas latviešu valodā tiek tulkots kā privātuma ietekmes novērtējums. Rīka mājaslapā ir teikts, ka šis rīks galvenokārt ir paredzēts datu kontrolieriem, kuri ir nedaudz pazīstami ar PIA procesu. [19] Tā ir *open source* programma, ko var lietot organizācijas serverī.

PIA rīks tika izstrādāts, balstoties uz trim principiem:

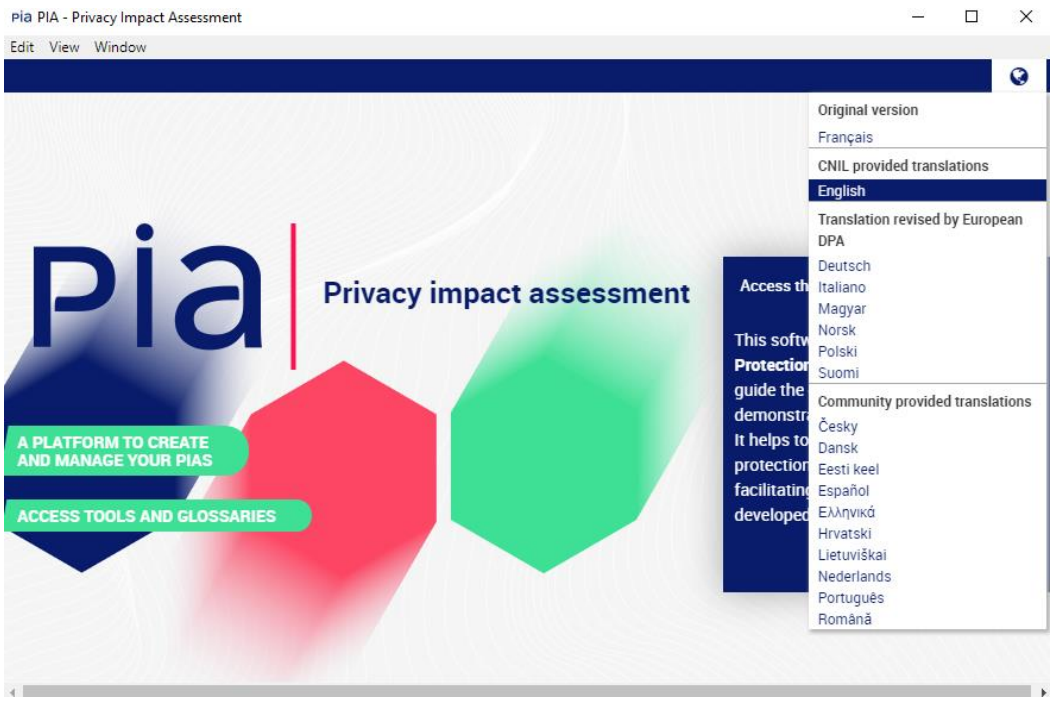
- Didaktisks interfeiss PIA veikšanai. Tas nozīmē, ka programmu ir viegli lietot.
- Juridisko un tehnisko zināšanu bāze. Tas satur informācijas bibliotēku ar VDAR un PIA rokasgrāmatu un CNIL drošības rokasgrāmatu datiem.
- Moduļu rīks. Tas nozīmē, ka to var pielāgot un izmainīt atbilstoši uzņēmuma prasībām, izmantojot bezmaksas licenci.

Lai autores izvēlētā uzņēmuma rīka apraksts nebalstītos tikai uz internetā pieejamo informāciju, autore nolēma to instalēt datorā, lai apskatītu un aprakstītu tā darbību un nolemtu, vai tas tiešām der uzņēmuma vajadzībām saistībā ar VDAR. Attēlā 5.1. var redzēt, kā rīks izskatās uzreiz pēc instalācijas. Tas sniedz informāciju par tā izstrādātājiem un mērķi, kāpēc tas tika izveidots.



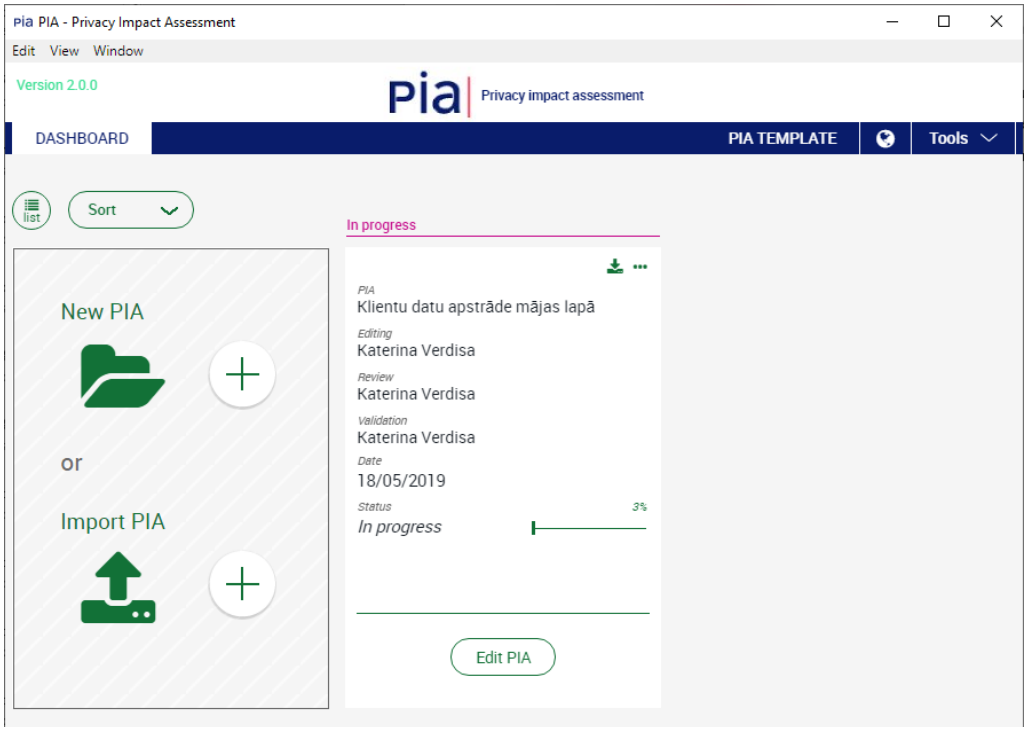
5.1. att. **PIA rīka logs pēc palaišanas.**

Rīkam ir pieejamas vairākas valodas, kā ir redzams attēlā 5.2. Kā saprata autore, šos tulkojumus piedāvā arī citi izstrādātāji vai rīka lietotāji, kas atrodas kopienā. Var redzēt, ka rīks satur divas Baltijas valstu valodas – lietuviešu un igauņu, bet ne latviešu. Autoresprāt, būtu vērts iztulkot šo rīku arī latviešu valodā, kas noderētu uzņēmuma vietējai filiālei, bet, tā kā apskatāmais uzņēmums ir starptautisks un datu kontrolieris atrodas Vācijā, var tikt izmantota angļu vai vācu valoda. Visas datnes, kas ir nepieciešamas rīka tulkošanai, ir pieejamas tā Git repozitorijā.



5.2. att. **PIA rīkam pieejamās valodas**

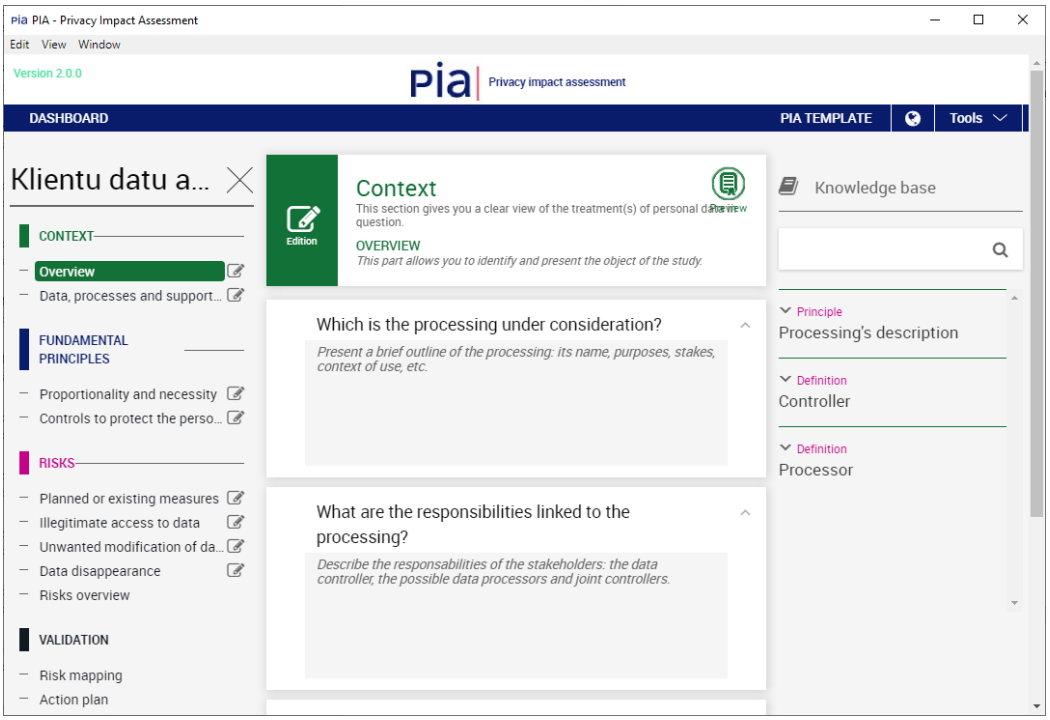
Rīks dod iespēju izveidot savu veidni ar konkrētu uzdevumu, kuru kontrolierim nepieciešams izskatīt. Autore kā piemēru izveidoja savu veidni, kas pārbaudīs, vai uzņēmuma mājaslapa atbilst regulas nosacījumiem. Tā ir redzama 5.3. attēlā.



5.3. att. **Veidnes izveide rīkā**

Rediģējot veidni, var redzēt ļoti daudz lauku, ko var aizpildīt ar nepieciešamo informāciju. To var redzēt 5.4. attēlā. Šie lauki ir :

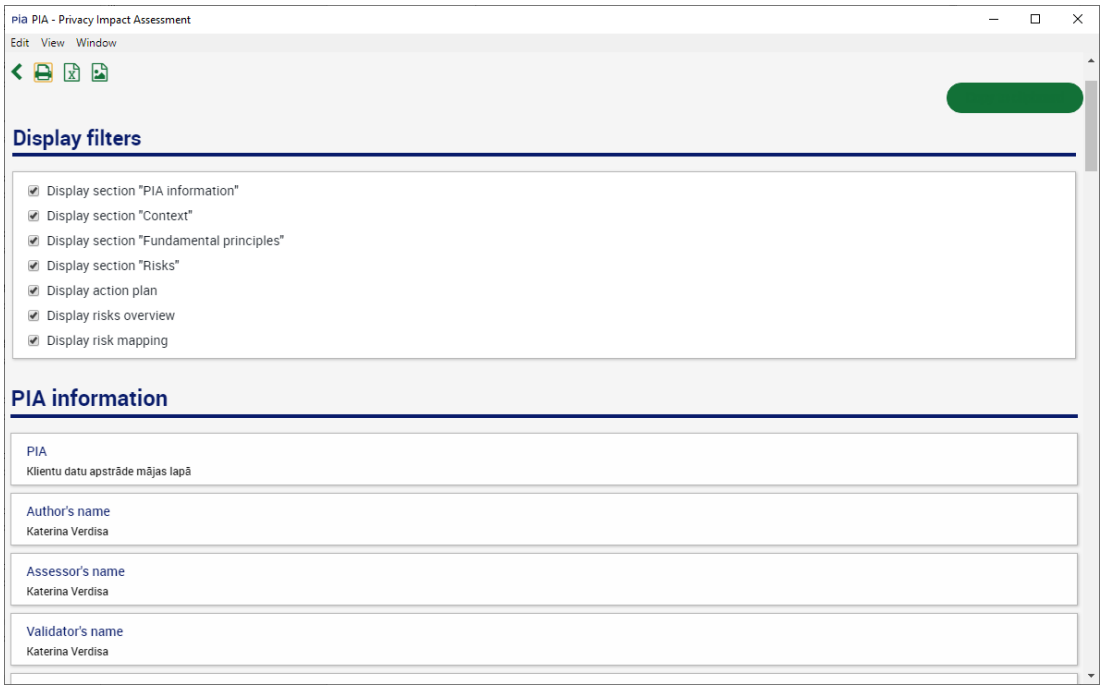
- **Konteksts –** šī sadaļa sniedz skaidru priekšstatu par attiecīgo personas datu apstrādi. Šajā sadaļā tiek aprakstīts objekts, kas tiks apskatīts, un dati, kas tajā tiek apstrādāti.
- **Pamatprincipi –** šī sadaļa ļauj izveidot konfidencialitātes principu atbilstības sistēmu.
- **Riski –** šī sadaļa ļauj novērtēt privātuma riskus, ņemot vērā esošās vai plānotās kontroles.
- **Apstiprināšana –** šī sadaļa ļauj sagatavot un formalizēt PIA validāciju.



5.4. att. **Veidnes apraksts rīkā**

Kā var redzēt 5.4. attēlā, rīka labajā pusē atrodas zināšanu bāzes nodaļa. Bāzē tiek sniegti definīciju skaidrojumi, kas atbilst katrai no sadaļām. Autoresprāt, nav ērti tas, ka nav iespējams meklēt uzreiz caur visu bāzi jebkurā no sadaļām. Piemēram, nav iespējams meklēt, ko nozīmē personas dati, atrodoties risku sadaļā. Bāze sniedz arī saites uz oficiālo VDAR mājaslapu.

Nospiežot pogu *Preview*, lietotājam rodas iespēja apskatīt visu veidni un tās saturu, kā arī to izdrukāt vai saglabāt nepieciešamos attēlus, piemēram, atskaitei. Tas redzams 5.5. attēlā.



5.5. att. **Veidnes priekšskatījums**

Kā autore novēroja, šīs rīks var palīdzēt arī projekta izstrādes laikā. Par katru projektu, kas ir saistīts ar e-komercijas produktu un datu apstrādi, var minēt, kādi dati tur tiks glabāti un vai tie ir drošībā. Vai arī to, kā tiks glabāti klienta dati saistībā ar katru jaunu projektu, kādi ir viņa datu izmantošanas nosacījumi utt. Autoresprāt, šis līdzeklis palīdzēs organizēt datu kontroliera darbu un digitālā veidā glabāt visu nepieciešamo informāciju par datu apstrādi.

Internetā ir pieejami dažādi rīki. Pārsvarā rīki ar labām atsauksmēm ir par maksu vai prasa uzņēmuma pārstāvja datus saziņai. Testējot šādus rīkus, autoresprāt, tie jāvērtē kritiski, jo to lietošana var radīt jaunas problēmas.

6. ZIŅOJUMU PĀRVALDĪBAS SISTĒMA

Līdz ar VDAR ieviešanu sāka rasties arī dažādi rīki un sistēmas, kuru izstrādātāji sola palīdzēt organizēt datu kontroliera darbību vai pielāgot organizēju darbību regulas prasībām. Arī autores apskatītais starptautiskais uzņēmums izmanto šādu sistēmu.

Uzņēmuma mājaslapā tiek publicētas dažādas ziņas par uzņēmumu un projektiem, kā arī reizi mēnesī tiek noformēts ziņojumu kopums, kas var tikt izsūtīts ieinteresētajām personām. Organizācija nolēma saviem klientiem piedāvāt iespēju pierakstīties uz saviem ziņojumiem savā mājaslapā. Šie ziņojumi tiks izsūtīti uz e-pastu, ko klients norādījis. Savukārt e-pasta adreses, ko uzņēmums sāk ievākt, tiek uzskatītas par personas datiem, ja tās satur personīgu informāciju, piemēram, klienta pārstāvja vārdu, kurš arī ir ES iedzīvotājs, tāpēc no šī brīža kļūst aktuāla VDAR.

Personai ir jāsniedz iespēja gan piekrist ziņojumu saņemšanai, tas ir, sava e-pasta apstrādei un glabāšanai, gan jebkurā laikā atteikties no pierakstīšanās. Principus, kas nodrošina šādu iespēju, sauc par *opt-in* (iestāšanās izvēles princips) un *opt-out* (izstāšanās izvēles princips). *Opt-in* nozīmē, ka jūs saņemsiet reklāmu vai ziņojumus tikai tādā gadījumā, ja būsiet lūguši nodrošināt šādu saziņu, piemēram, nospiežot pogu ar saiti uz piekrišanu. *Opt-out* nozīmē**,** ka jūs varat atteikties no komerciālo ziņojumu saņemšanas.

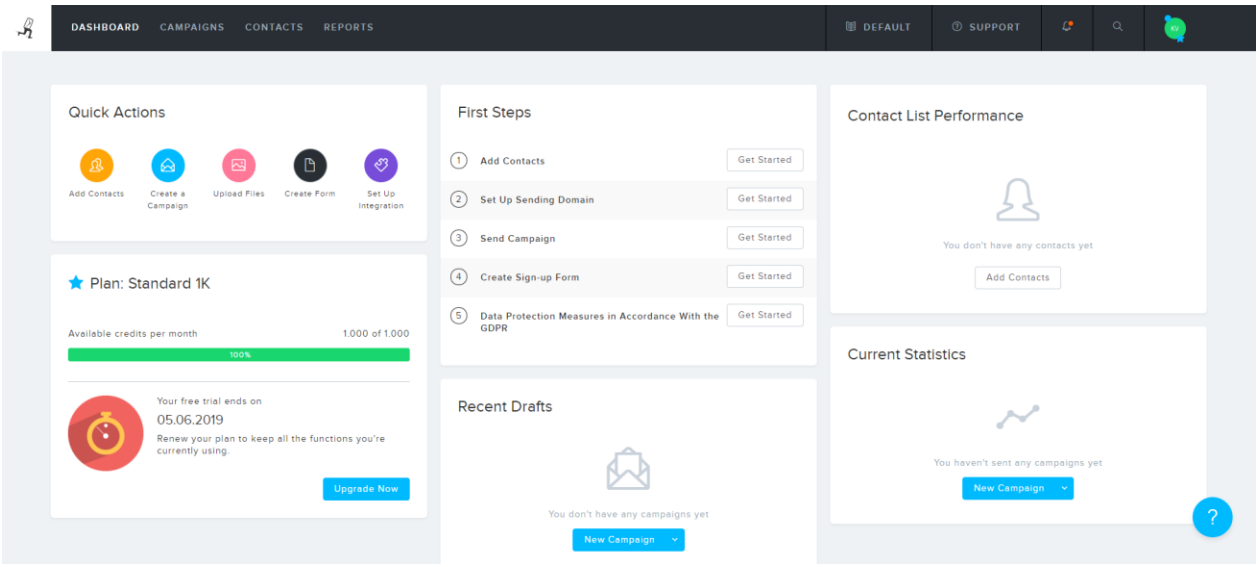
Darbā apskatītais starptautiskais uzņēmums izmanto *Newsletter2Go* sistēmu. Tā ir tīmekļa e-pasta mārketinga sistēma. [20] Tās mērķis ir atvieglot komerciālo e-pastu sūtīšanu un noformēšanu, ceļot uzņēmuma mārketinga kvalitāti. Šī sistēma sola efektīvu ziņojuma veidņu izveidi, kas neprasa zināšanas programmēšanā, sertificētu datu aizsardzību un integrāciju ar e-komercijas, CRM un CMS sistēmām.

Lai izskatītu šo sistēmu un iegūtu bezmaksas laicīgu piekļuvi, autorei tajā bija nepieciešams reģistrēties. Interesanti ir tas, ka sistēma neļauj reģistrēties personām ar bieži sastopamām e-pasta adresēm. Piemēram, autore nevarēja reģistrēties ar savu *Gmail* e-pastu, jo sistēma prasīja uzņēmumam piederošu e-pastu un saziņas datus. Pēc reģistrēšanās uzreiz kļuva iespējams apskatīt sistēmu, bet sistēmas augšā bija paziņojums, ka autores datu atbilstība tiks pārbaudīta apmērām divu stundu laikā.

Ielogojoties saitē, nosaukumam pievienojas “ui”, kas nozīmē lietotāja saskarni. Tās izskatu var redzēt attēlā 6.1. Var redzēt, ka sistēma piedāvā dažādas ātras darbības:

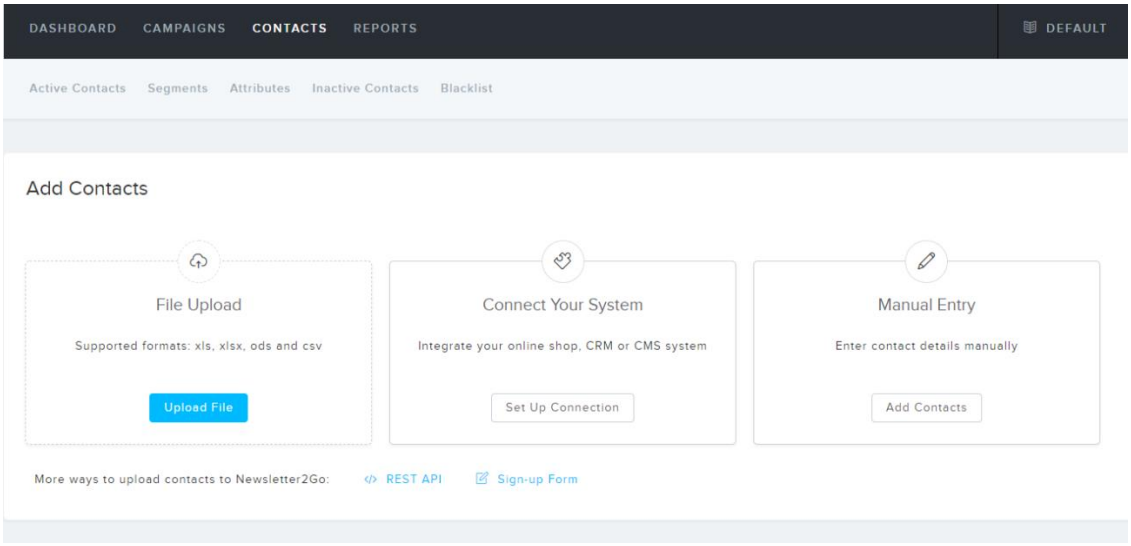
- pievienot kontaktus
- izveidot kampaņu
- augšupielādēt datnes
- izveidot veidlapu
- izveidot integrāciju

Tāpat tiek piedāvāti pirmie soļi, kas jāveic, pirms sūtīt ziņojumus. Kā var redzēt, 5. solis ir Datu aizsardzības pasākumi saskaņā ar VDAR, kas autori jo īpaši interesē, jo ar to ir saistīta šī darba tēma.



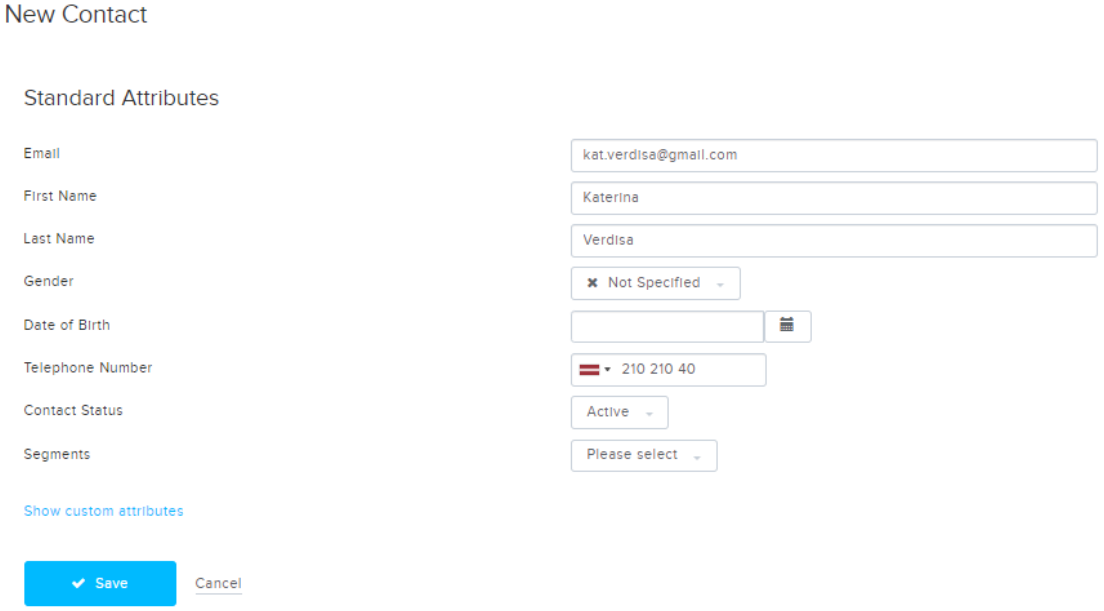
6.1. att. ***Newsletter2Go* sistēmas lietotāja saskarnes galvenā lapa.**

Vispirms autore apskatīja, kādā veidā var pievienot kontaktus, kam tiks izsūtīti ziņojumi. Kā var redzēt attēlā 6.2., kontaktus var pievienot, ielādējot datnes ar konkrētu formātu, pieslēdzot CRM, CMS vai e-komercijas sistēmas, kā arī manuāli ievadot klientu e-pastus. Lai arī *Newsletter2Go* izstrādātāji raksta, ka nav jābūt programmēšanas prasmēm, lai lietotu šo sistēmu, viņi tāpat piedāvā iespēju izmantot API, kas ir lietojumprogrammas saskarne. Sistēma satur lielu API dokumentācijas bāzi, lai klients pats varētu izveidot to, kas viņam nepieciešams. Palaist API rediģēšanas iespēju sistēma piedāvā ar *Postman* rīku, savukārt sistēmas izmantotā programmēšanas valoda ir JSON. [21]



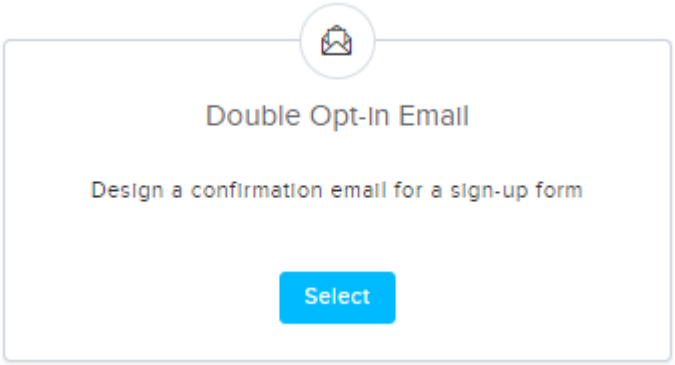
6.2. att. ***Newsletter2Go*** **sistēmas lietotāja saskarnes galvenā lapa.**

Autore izvēlējas izveidot kontaktu manuāli. Attēlā 6.3. ir redzams, kādus personas datus ir iespējams ievadīt, reģistrējot jauno klientu. Autore pamanīja, ka sistēma spēj pārbaudīt, cik pareizi ir ievadīts numurs. Piemēram, nebija iespējams ievadīt Latvijas numuru, sākot ar ciparu, kas nav 2, vai kura ciparu skaits ir mazāks par astoņi. Taču, autoresprāt, sistēmas izstrādātajiem ir jāpievērš uzmanība personas dzimšanas gadam, jo regulā ir skaidri noteikts par personas, kas nav sasniegusi 16 gadus, datu izmantošanu. Atļauju izmatot šīs personas datus var sniegt tikai tās vecāki, tāpēc, pēc autores domām, aizpildot dzimšanas datuma aili, var brīdināt, ka persona nav sasniegusi 16 gadu vecumu.



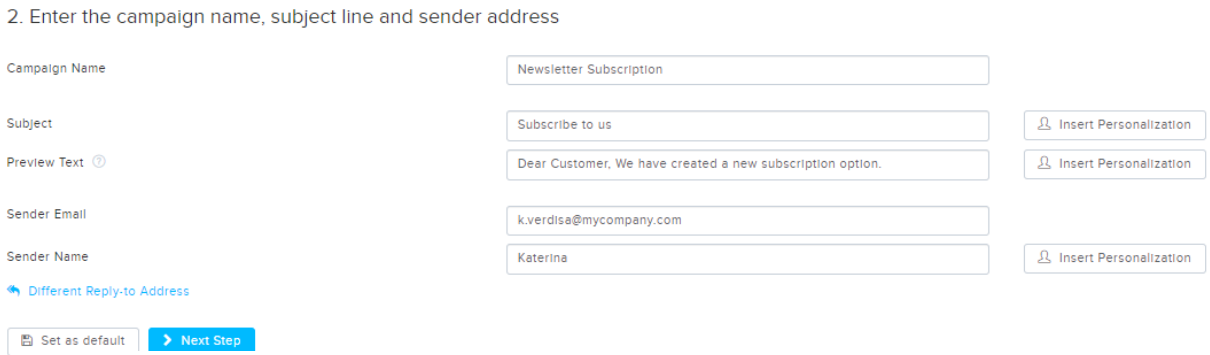
6.3. att. ***Newsletter2Go*** **sistēmas lietotāju pievienošana.**

Nākamais solis ir pierakstīšanās ziņojumam izveidot piekrišanas veidni un nosūtīt e-pastu izveidotajam kontaktam. Jādodas uz kampaņas sadaļu un jāizvēlas dubultais *opt-in* e-pasts, kā ir redzams 6.4. attēlā. Dubultā izvēles e-pasta ziņojumā ir apstiprinājuma saite, ko uzņēmuma kontaktpersonas var izmantot, lai pierakstītos ziņojumiem.



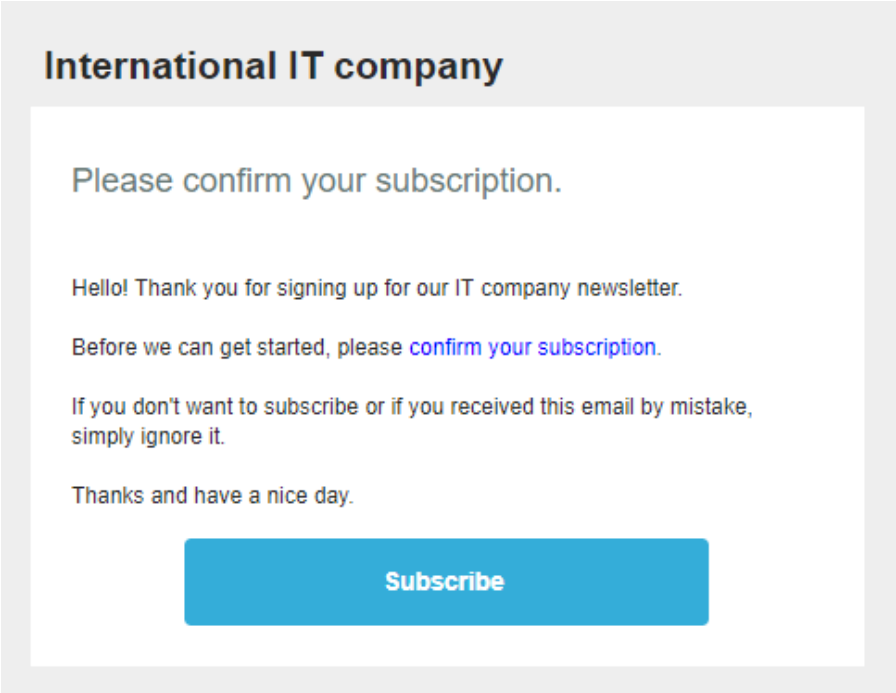
6.4. att. ***Newsletter2Go*** **ziņojumu piekrišanas** ***Double Opt-in Email*** **veidnes izvēle**

Nākamais solis ir aizpildīt pierakstīšanās kampaņas veidlapā nepieciešamo informāciju, kā var redzēt 6.5. attēlā. Autore aizpildīja to ar kampaņas nosaukumu, priekšmetu, tekstu, sūtītāja e-pastu un vārdu. Dažus laukus var personalizēt, padarot tos īpašus. Var pat izveidot īpašu saturu, izmantojot loģiskus programmēšanas priekšrakstus *if/then/overwise*. Piemēram, ja klienta e-pasts satur kādu vārdu, tad viņš saņems citu kampaņas nosaukumu vai citu sūtītāja vārdu. Pēc autores domām, to ir ērti izmantot, piemēram, ja ir vairākas valodas.



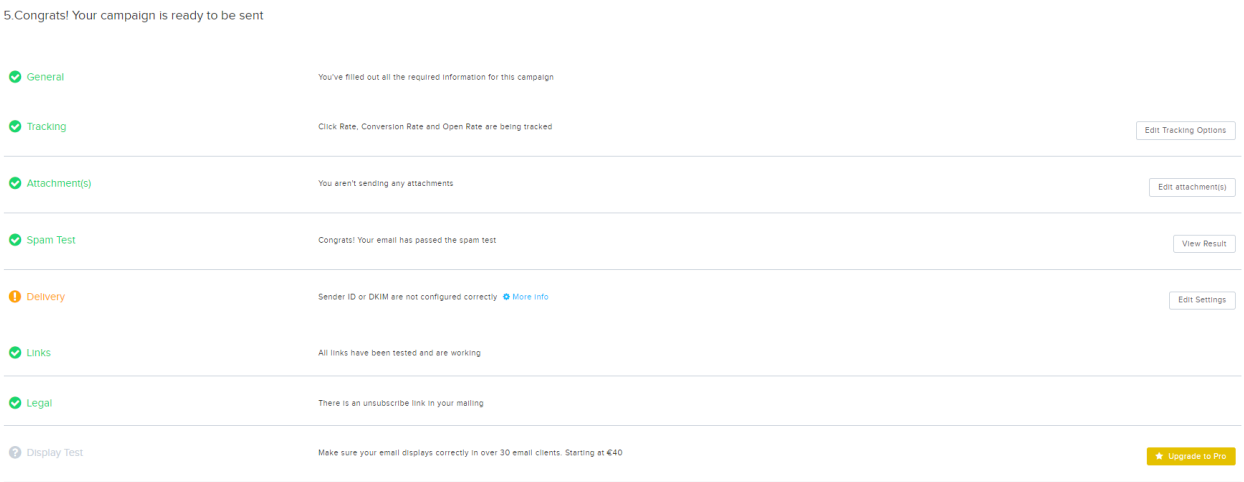
6.5. att. ***Newsletter2Go*** **ziņojumu piekrišanas veidnes informācijas lauki**

Tad autore izvēlējas veidnes izskatu, ko lietotāji var rediģēt pēc saviem ieskatiem. Vēl sistēma sniedz iespēju ielādēt vai iekopēt savu datni ar HTML kodu. Autore izveidoja savu piemēru, izmantojot gatavo veidni, ko var redzēt 6.6. attēlā .



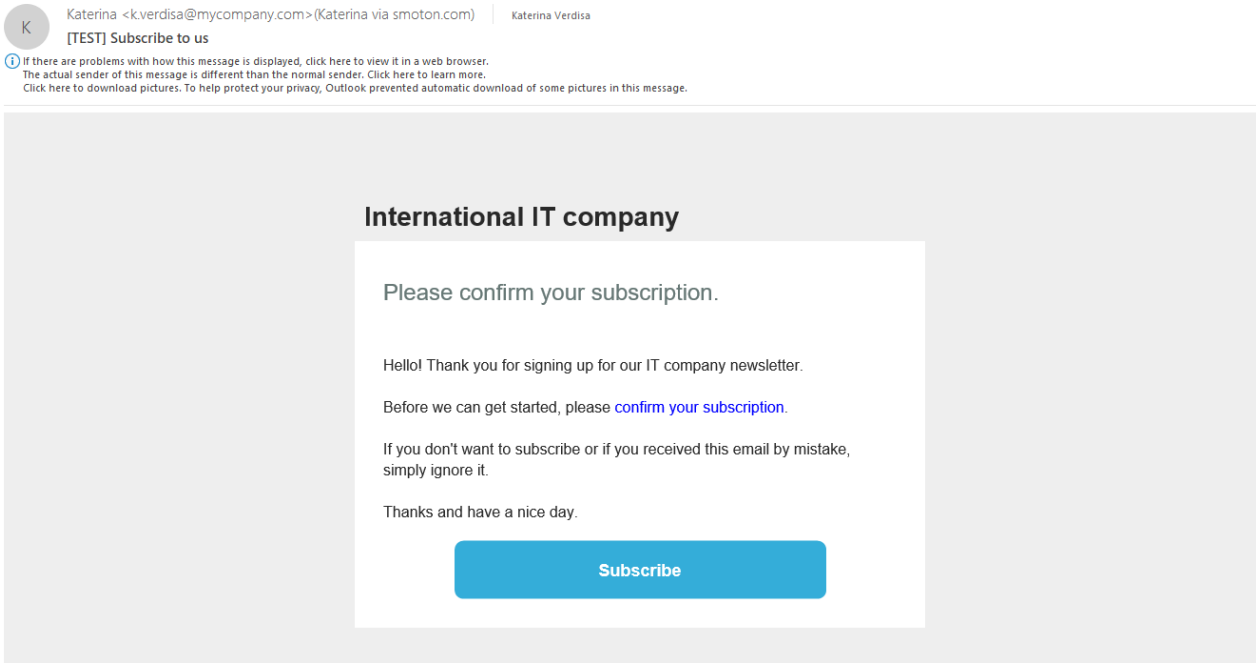
6.6. att. ***Newsletter2Go* ziņojumiem izveidota veidne**

Nākamajā solī ir redzams atgādinājums, kas lietotājam dod iespēju pārbaudīt, vai visas darbības ir veiktas un visi laukumi ir aizpildīti, ko var apskatīt 6.7. attēlā. Pastāv iespēja pat pārbaudīt, vai šī vēstule tiks uzskatīta par spamu jeb nevēlamu e-pastu. Kā redzams pēc testa palaišanas, vēstule netiks piegādātā kā nevēlams e-pasts.



6.7. att. ***Newsletter2Go* ziņojumu noformējuma pārbaude**

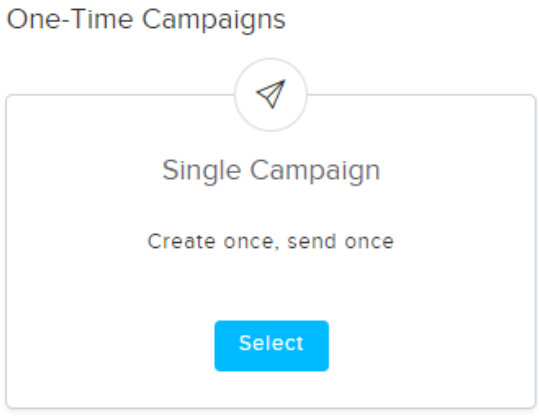
Pēc pārbaudes ziņojums tika nosūtīts uz kontaktu e-pastu. Attēlā 6.8. ir redzams, kā izskatās ziņojums, kad tas ir nonācis klienta e-pastā. Visas saites ir uzklikšķināmas, bet pagaidām ved uz oficiālo *Newsletter2Go* mājaslapu ar speciālu sadaļu *Subscribe*, taču tā kā visām saitēm un pogām uzņēmums spēja pievienot savas saites, tās strādā pareizi.



6.8. att. ***Newsletter2Go* ziņojumu piekrišanas klienta e-pastā.**

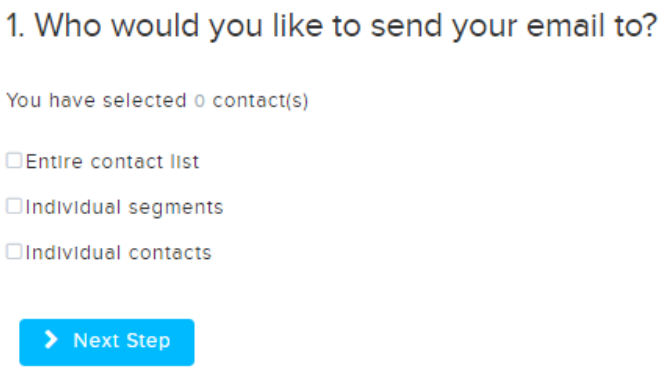
Pēc tam, kad klientam radās iespēja pierakstīties ziņojumiem, autore nolēma, ka ir nepieciešams pārbaudīt, kā tiek veidoti kampaņas ziņojumi un vai saņēmējiem ir iespēja no tiem atteikties.

Lai izveidotu kampaņas veidlapu, jāaiziet uz kampaņas sadaļu un jāizvēlas no piedāvātajiem. Autore izvelējas vienreizējo kampaņu, kā var redzēt 6.9. attēlā, kas tiks sūtīta tikai vienu reizi.



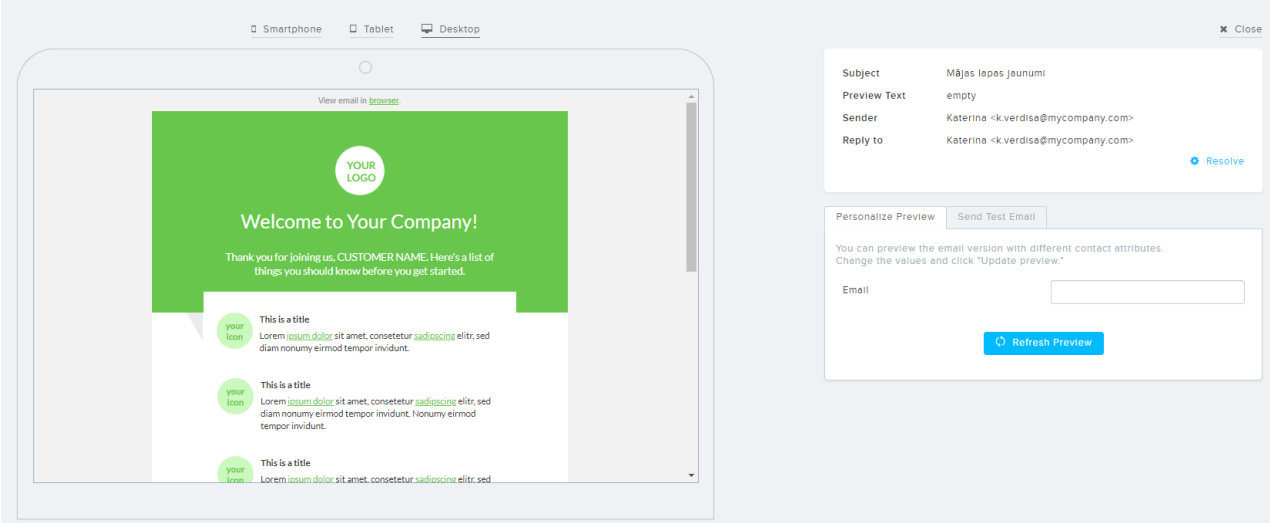
6.9. att. ***Newsletter2Go* vienreizējas kampaņas izvēle**

Ir jāsāk ar kontaktu sarakstu, kam tiks izsūtīts ziņojums, kā attēlots 6.10. attēlā. Autore izvēlējas individuālu kontaktu un ievadīja sava e-pasta datus.



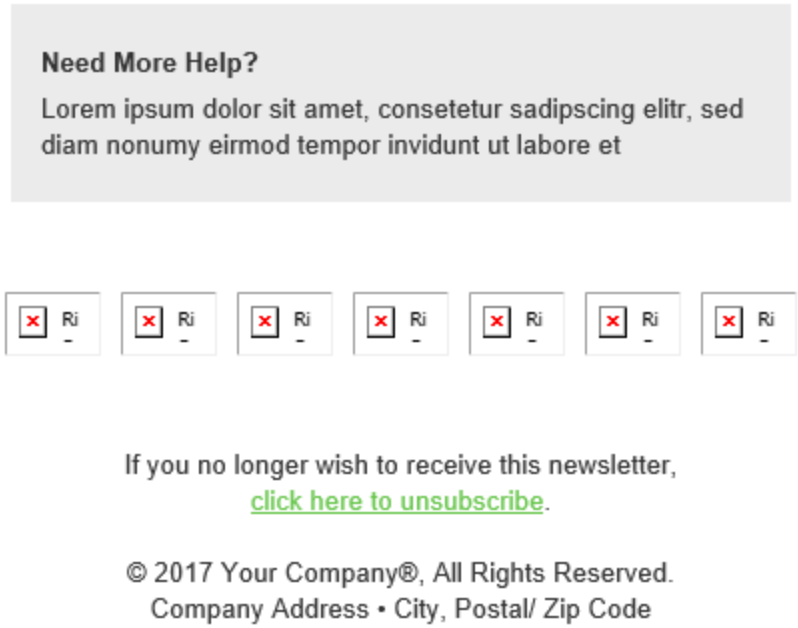
6.10. att. ***Newsletter2Go*** **vienreizējas kampaņas kontaktu izvēle**

Nākamajā solī ir jānoformē veidnes teksts, kas līdzinās piekrišanas izveidei, un tad jāizvēlas veidnes dizains. *Newsletters2Go* piedāvā plašu dizaina izvēli, kā arī var izmantot savējo, ielādējot datni ar HTML kodu. Autore izvelējas dizainu, kas ir redzams 6.11. attēlā. Var aplūkot, kā ziņojuma noformējums izskatīsies arī uz citam ierīcēm.



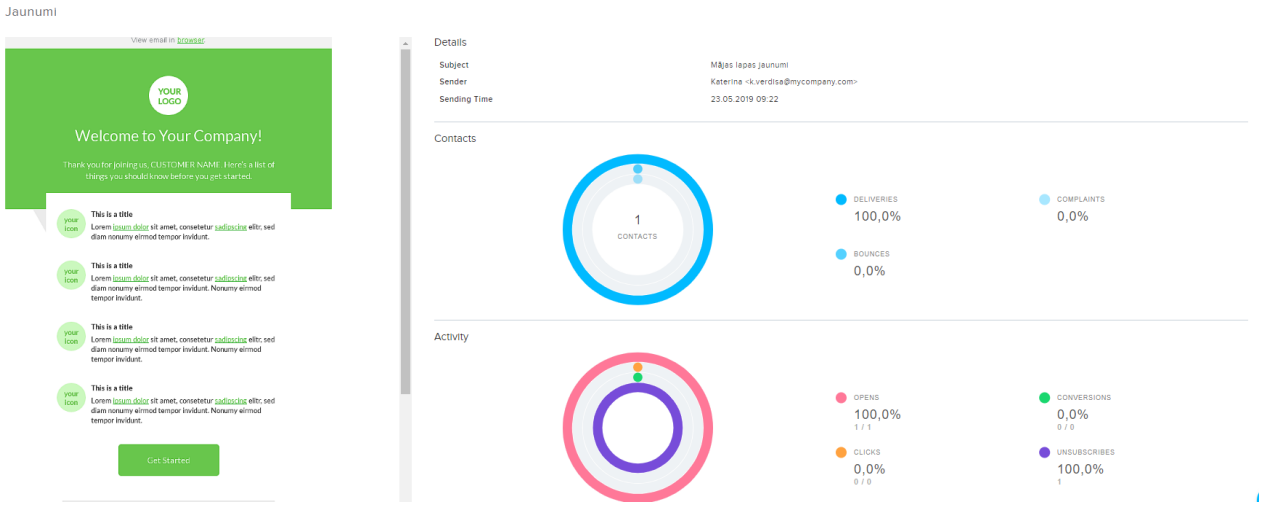
6.11. att. ***Newsletter2Go*** **vienreizējas kampaņas kontaktu izvēle**

Pēdējais solis ir ziņojuma nosūtīšana. Sistēma paziņo, ka ziņojums tiks nosūtīts pēc apstrādes. Pēc veiksmīgas ziņojuma nosūtīšanas autore uzreiz pārbaudīja, vai ziņojuma beigās ir iespēja atteikties no ziņojumu saņemšanas. Kā var redzēt attēlā 6.12., klients var nospiest uz saites, lai atrakstītos no ziņojumiem.



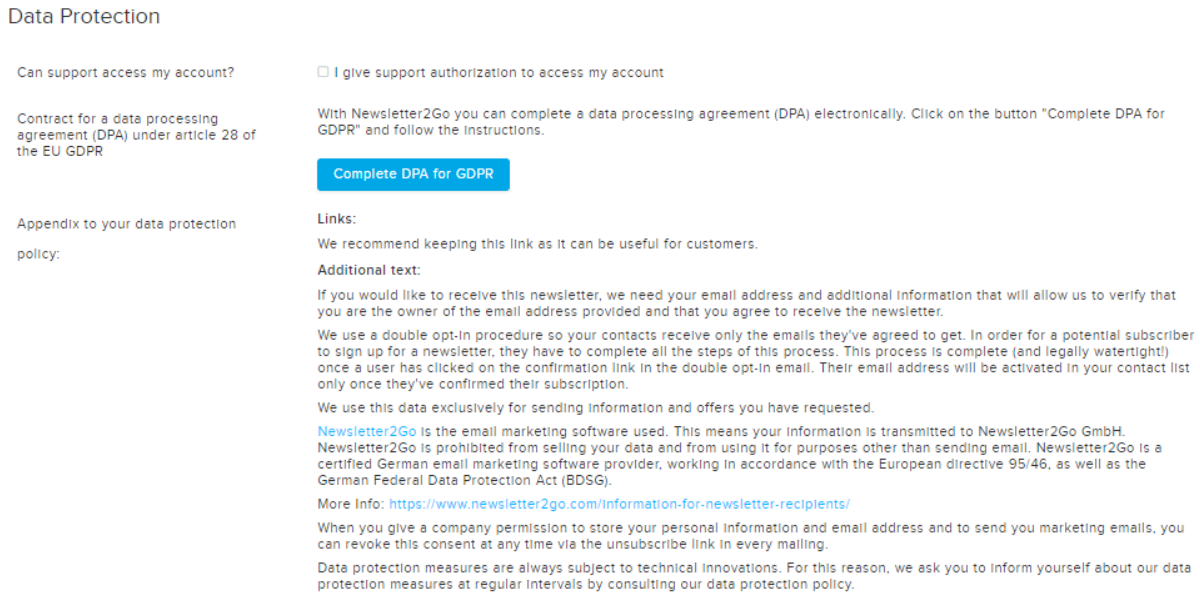
6.12. att. ***Newsletter2Go* klientu izvēle atteikties no ziņojumiem**

Newsletters2Go piedāvā iespēju arī apskatīt statistiku saistībā ar savām kampaņām. Uzreiz, kad autore atteicās no ziņojumu saņemšanas, uzņēmuma administratoram kļuva redzams, ka viena persona ir atteikusies no ziņojumiem, bet sistēma nerāda, kas tā ir par personu. To var redzēt attēlā 6.13. – ar violetu krāsu iezīmētais riņķis.



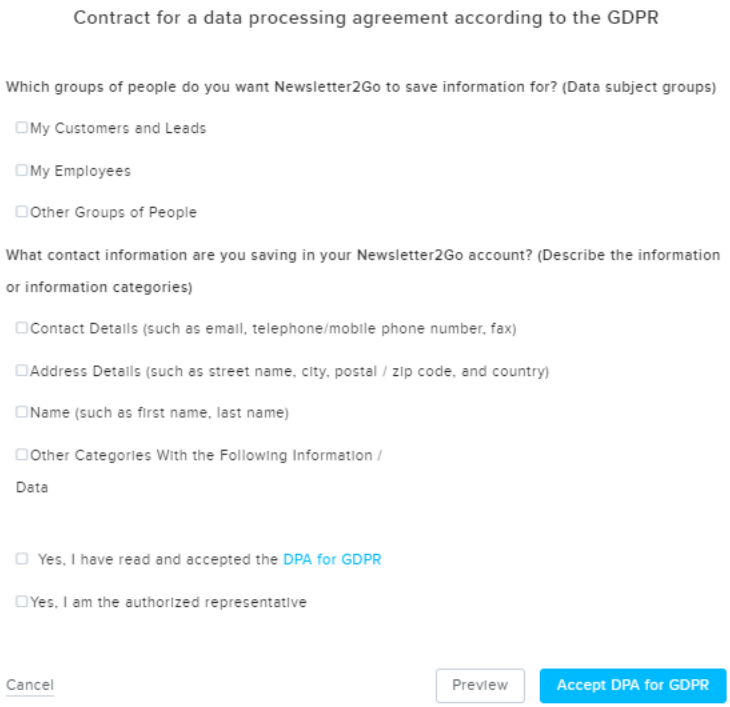
6.13. att. ***Newsletter2Go* ziņojumu statistikas dati**

Pēdējais no piedāvātajiem soļiem sistēmā ir datu aizsardzības pasākumi saskaņā ar VDAR. Sadaļu var apskatīt 6.14. attēlā. Šis solis visvairāk ieinteresēja autori ar savu saturu.



6.14. att. ***Newsletter2Go*** **datu aizsardzības nosacījumi**

To apskatot, autore iepazinās ar lietotāja iespējam piekrist sistēmas atbalstītajiem piekļūt administratora lomai. Nākamais, kam tiek pievērsta lietotāja uzmanība, ir elektroniskās piekrišanas datu apstrādei ar *Newsletters2Go*. Piekrišanu var apskatīt 6.15. attēlā.



6.15. att. ***Newsletter2Go*** **datu apstrādes līgums**

Vēl sistēmas izstrādātāji piedāvā nokopēt un ievietot savas mājaslapas datu aizsardzības nosacījumus par to, ka datu apstrāde notiek ar šīs sistēmas palīdzību un ka tā nedrīkst pārsūtīt datus citām personām. Darba 4.2. nodaļā tika minēts, ka šis teksts tiek izvietots arī starptautiskā uzņēmuma mājaslapā kā viens no datu drošības nosacījumiem.

Testējot *Newsletters2Go* sistēmu, autorei par to izveidojās savs iespaids. Pirmkārt, šī sistēma ir ļoti ērta. Sistēmas saskarni ir viegli izmantot, un ar laiku lietotājs to varēs darīt intuitīvi, un, ja ir nepieciešams, sistēma dod iespēju uzprogrammēt to, ko pats lietotājs vēlas. Otrkārt, sistēmā ir ļoti daudz gatavu dizaina veidņu, kā arī ir iespēja ielādēt savējo, padarot efektīvu uzņēmuma mārketingu. Treškārt, sistēma satur ļoti daudz pamācību un dokumentāciju, kas ir detalizēti aprakstīta. Ceturtkārt, sistēmā ir pieejama statistika par ziņojumu izsūtīšanu, kas ir ērti attēlota. Piektkārt, sistēma sniedz lietotajam vienošanos par drošu klientu datu glabāšanu un apstrādi un atbilst VDAR nosacījumiem. Vienīgais mīnuss ir tas, ka sistēma neseko lietotāju klientu dzimšanas gadam un tā varētu brīdināt par to, ka šim klientam būs nepieciešams papildus apstiprināt savu datu izmantošanu, saņemot vecāku piekrišanu, ja persona nav sasniegusi 16 gadu vecumu. Uzņēmuma darbinieki, kas strādā ar sistēmu, piekrīt autores viedoklim par sistēmas ērtību, tāpēc autore ieteiktu turpināt ar to strādāt.

IEGŪTIE REZULTĀTI

Darba rezultātā tika izpētīta Vispārīgā datu aizsardzības regula, tās ieviešanas iemesls un mērķis, kā arī regulas aizsargātie dati. Tika apskatīta regulas tapšanas vēsture un ieviešana Latvijas Republikā.

Tika apskatīta regulas nepieciešamība tieši IT uzņēmumā un uzskaitīti iemesli, kāpēc sistēmas, kura izmantos personas datus, izstrādātajiem ir jāiepazīstas ar regulas nosacījumiem.

Autore izpētīja un salīdzināja regulas ieviešanas ietekmi un tās radītās izmaiņas gada laikā starptautiskā IT uzņēmumā. Lai veiksmīgi apskatītu pareizu regulas pielietojumu uzņēmumā, praktiskajā daļā autore izstrādāja vadlīnijas, kurām var veiksmīgi sekot, testēja un ieteica uzņēmumam vienu datu kontroles rīku un iepazinās ar uzņēmumā izmantoto sistēmu, kuru ieviesa līdz ar regulu un kuras uzdevums ir pārsūtīt ziņojumus klientiem pēc viņu piekrišanas.

Visbeidzot autore piedalījās regulas ieviešanā uzņēmumā un iekšējo noteikumu izstrādē, uzstājoties ar pašas veidotu prezentāciju, lai iepazīstinātu uzņēmuma Latvijas filiāles darbiniekus ar jauno regulu un viņu tiesībām.

SECINĀJUMI

Darba izstrādes gaitā tika izdarīti šādi secinājumi:

1. Vispārīgā datu aizsardzības regula bija nepieciešama sakarā ar jauno tehnoloģiju ietekmi uz personas datu apstrādi un glabāšanu, kas pēdējos gados notiek elektroniskā veidā. Personas datu izmantošana internetā, īpaši sociālajos tīklos, iepriekš īpaši netika regulēta.

2. Datu aizsardzības princips Latvijas Republikā nemainījās. Balstoties uz regulas nosacījumiem, tika pieņemts un stājas spēkā jauns Personas datu apstrādes likums. Paplašinājās datu subjektu tiesības. Juridiskās personas kļuva brīvākas no Datu valsts inspekcijas, un tagad tām pašām ir jāorganizē datu drošības pasākumi un jāvēršas Datu valsts inspekcijā tikai pārkāpumu gadījumos.

3. Vispārīgā datu aizsardzības regula ir pielietojama jebkurā uzņēmumā, kas strādā ar personas datiem. IT uzņēmumam tās pielietojums atšķiras ar to, ka uzņēmuma darbiniekiem jābūt plašāk informētiem par tās noteikumiem, ja tie nodarbojas ar tādu sistēmu izstrādi, kas ir saistīta ar datiem.

4. Starptautiskā IT uzņēmumā jāievēro ne tikai VDAR noteikumi, bet katrai filiālei vēl papildus jāievēro nacionālie likumi saistībā ar datu aizsardzību. Ievelētajam datu pārzinim ir jābūt ērti pieejamam katrā no filiālēm, kur strādā ES pilsoņi un nepilsoņi.

5. Gada laikā situācija darbā apskatītajā uzņēmumā saistībā ar VDAR implementāciju ir uzlabojusies. Uzņēmums grasās organizēt darbinieku apmācības un izsūtīt darbiniekiem piekrišanas saistībā ar viņu datiem. Uzņēmuma oficiālajā mājaslapā paradījās nosacījumi par datu drošību personām, kuras vēlas sūtīt savus datus, lai pieteiktos darbā, vai klientiem, kuri vēlas pierakstīties ziņojumiem. Šie nosacījumi ir saprotami un kodolīgi. Diemžēl iekšējais datu drošības regulējums joprojām nav pieejams angļu valodā un personāls joprojām nav apmācīts un iepazīstināts ar datu pārzini.

6. Uzņēmuma mājaslapā tiek izmantota sistēma *Newsletter2Go*, kuras uzdevums ir klientu datu glabāšana un ziņojumu izsūtīšana. Sistēmai ir ērta lietotāju saskarne, un tās darbības princips atbilst VDAR prasībām. Pēc vēlēšanās tai ir pieejama dokumentācija, kuru izmantojot lietotājs var uzprogrammēt nepieciešamās funkcijas.

7. Autores izstrādātās vadlīnijas var noderēt jebkuram IT uzņēmumam. Tā kā darbā apskatītajā uzņēmumā situācija ar VDAR joprojām nav pilnīgi apmierinoša, tas var izmantot šīs vadlīnijas un salīdzināt ar veiktajām darbībām saistībā ar regulas ieviešanu, kā arī pārbaudīt iekšējā regulējuma atbilstību.

IZMANTOTA LITERATŪRA UN AVOTI

1. Global digital population as of January 2019 (in millions). [tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: https://www.statista.com/statistics/617136/digital-population-worldwide/

2. New York Daily News. [tiešsaite]. - [atsauce 20.04.2019]. Pieejams Internetā: https://www.tribpub.com/gdpr/nydailynews.com/

3. GDPR: Tech firms struggle with EU's new privacy rules. [tiešaite]. – [atsauce 20.04.2019] Pieejams Internetā: https://www.bbc.com/news/technology-44239126

4. Datu valsts inspekcijas rekomendācija „Personas datu definīcija". [tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: https://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Personas_datu_definicija_rekomendacija.pdf

5. Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (Dokuments attiecas uz EEZ) [tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32016R067

6. Brikmane, E. - Kas ir personas dati? Vispārīgā datu aizsardzības regula I. [tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: https://lvportals.lv/skaidrojumi/294871-kas-ir-personas-dati-vispariga-datu-aizsardzibas-regula-i-2018

7. Datu valsts inspekcija. Personas datu aizsardzība. Vispārīgā datu aizsardzības regula. [tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: https://www.dvi.gov.lv/lv/wp-content/uploads/1_Personas-datu-aizsardz%C4%ABba_Visp%C4%81r%C4%ABg%C4%81-datu-aizsardz%C4%ABbas-regula_20032018.pdf

8. Birkmane, E. - Personas dati un Vispārīgā datu aizsardzības regula. [tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: https://lvportals.lv/viedokli/292782-personas-dati-un-vispariga-datu-aizsardzibas-regula-2018

9. Eiropas Savienības Pamattiesību harta. Eiropas Savienības Oficiālais Vēstnesis C 326/391.[tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A12012P%2FTXT

10. Fizisko personu datu aizsardzības likums: LR likums. "Latvijas Vēstnesis", 123/124 (2034/2035), 06.04.2000., [tiešsaiste] - [atsauce 20.04.2019] - http://likumi.lv/doc.php?id=4042.

11. Latvijas Administratīvo pārkāpumu kodekss: LR likums.. "Ziņotājs", 51, 20.12.1984. [tiešsaiste]. - [atsauce 20.04.2019]. Pieejams Internetā: http://likumi.lv/doc.php?id=89648

12. Stājas spēkā jaunais Fizisko personu datu apstrādes likums. [tiešsaiste]. - [atsauce 22.04.2019]. Pieejams Internetā: https://lvportals.lv/skaidrojumi/297136-stajas-speka-jaunais-fizisko-personu-datu-apstrades-likums-2018
13. Vadlīnijas par tiesībām uz datu pārnesamību. [tiešsaiste]. - [atsauce 22.04.2019]. Pieejams Internetā:http://www.dvi.gov.lv/lv/wp-content/uploads/WP-242_Vadl%C4%ABnijas-par-ties%C4%ABb%C4%81m-uz-datu-p%C4%81rnesam%C4%ABbu.pdf
14. Libeka, M. Latvijas Āvīze. Tiesības tikt aizmirstam un izdzēstam. [tiešsaiste]. - [atsauce 22.04.2019]. Pieejams Internetā: http://www.la.lv/tiesibas-tikt-aizmirstam-un-izdzestam/
15. Eiropas Komisija. Kas ir datu aizsardzības pārkāpums un ko darīt, ja šāds pārkāpums noticis? [tiešsaiste]. - [atsauce 22.04.2019]. Pieejams Internetā: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_lv#piemri
16. Fizisko personu datu apstrādes likums. [tiešsaiste]. –
[atsauce 22.04.2019]. Pieejams Internetā: https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums
17. Pamatnostādnes administratīvo naudas sodu piemērošanai un noteikšanai Regulas 2016/679 vajadzībām. [tiešsaiste]. - [atsauce 22.04.2019]. Pieejams Internetā: https://www.dvi.gov.lv/lv/wp-content/uploads/Pamatnost%C4%81dnes-administrat%C4%ABvo-naudas-sodu-piem%C4%93ro%C5%A1anai-un-noteik%C5%A1anai-LV.pdf
18. European Comiccion. EU-US Privacy Shield. [tiešsaiste]. – [atsauce 17.05.2019]. Pieejams Internetā: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en
19. The open source PIA software helps to carry out data protection impact assesment. [tiešsaite]. – [atsauce 17.05.2019]. Pieejams Internetā: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
20. About Newsletter2Go. [tiešsaite]. – [atsauce 22.05.2019]. Pieejams Internetā: https://www.newsletter2go.com/about-newsletter2go/
21. Newsletter2Go API [tiešsaite]. – [atsauce 22.05.2019]. Pieejams Internetā:
https://docs.newsletter2go.com/?_ga=2.102342593.1997214164.1558533012-1460051233.1558533012&version=latest#getting-started

PIELIKUMS

1. pielikums. Prezentācija uzņēmuma darbinieku apmācībām par VDAR

WHY GDPR?

The relevance of the personal data processing has increased exponentially. That happened because of the development of the digital marketing.

Data collection, storage, analysis and transfer has become more effective and easy thanks to modern technologies.

New technologies, Internet and electronic means of payment create new posibilities to collect data and new opportunities for their use.

WHAT ARE PERSONAL DATA?

Personal Data is data by which human beings can be identified.

These human beings are called data subjects.

Data protection serves the protection of data subjects and their rights.

Personal data are:

- name and surname;
- home address;
- email address with your name and surname;
- identification card number;
- location data;
- IP address;
- etc.

Sensitive personal data are:

- racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- person's sex life or sexual orientation.

NOT personal data are:

- company registration number;
- company email address;
- anonymized data.

Data Subjects' Rights

the right to be informed

the right of access

the right to rectification

the right to erasure

the right to restrict processing

the right to data portability

the right to object to processing

Example

Google Confirms It Will Automatically Delete Your Data -- What You Need To Know

Davey Winder Contributor

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

"You can already use your Google Account to access simple on/off controls for Location History and Web & App Activity," they say, "and if you choose, to delete all or part of that data manually."

What's new is the soon to be rolled out "auto-delete controls" that will enable users to set time limits on how long Google can save your data.

Link: https://www.forbes.com/sites/daveywinder/2019/05/05/google-confirms-it-will-automatically-delete-your-data-what-you-need-to-know

Principles of personal data processing

Lawfulness, fairness and transparency

Purpose limitation

Data minimization

Accuracy

Storage limitation

Integrity and confidentiality

Principles of personal data processing

Lawfulness, fairness and transparency

Data processing must be **lawful, fair and transparent**.

Purpose limitation

Data may **only** be collected and processed for those **specific, explicit and legitimate purposes** that have been **stated**.

Data minimization

Data must be **minimized** to what is necessary **in relation to the purpose**. If data are not necessary anymore, they should be **erased.**

Principles for processing of personal data

Accuracy

There must be **no mistakes** in the personal data.

Storage limitation

Data should be **deleted** when they are no longer needed.

Integrity and confidentiality

Personal Data must be **confidential, protected** and may **not be transferred to third parties** without agreement.

Example

Chat app Knuddels fined €20k under GDPR regulation

November 24, 2018 By Pierluigi Paganini

The case is making the headlines, the German chat platform Knuddels.de ("Cuddles") has been fined €20,000 for storing user passwords in plain text.

In July hackers breached the systems of the company Knuddels and leaked online its data.

In September, an unknown individual notified Knuddels that crooks published user data of roughly 8,000 members on Pastebin and much more data were leaked via Mega.nz.

Knuddels published a data breach notification and forced users into changing passwords, Knuddels also reported the incident to the Baden-Württemberg data protection authority.

The company duly notified its users and the Baden-Württemberg data protection authority.

Link: https://securityaffairs.co/wordpress/78393/laws-and-regulations/knuddels-gdpr-fines.html

STEPS FOR GDPR IMPLEMENTATION

Data security provision

Data audit

Employee training

Data subjects' consent to data processing

Data subjects' rights support

Be prepared for breaches

GDPR FOR DEVELOPERS

Since developers usually are the people who create data processing and storing programs, it is necessary to know the requirements of the GDPR, because they impact the business processes and architectural roadmaps for any software, system or application.

They must know how to correctly design the development of business processes for products and services and prepare their system to comply with all users' GDPR rights.

"Having the right mindset towards data protection helps to future proof a business.

It will put it in the right place to keep up with legislation."

-Elizabeth Denham

the UK Information Commissioner at the ICO

Thank you!

Questions?

Bakalaura darbs “Vispārīgas datu aizsardzības regulas pielietojuma apskats starptautiskā IT uzņēmumā” izstrādāts Latvijas Universitātes Datorikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Katerīna Verdiša _____ 27.05.2019.

Rekomendēju/nerekomendēju darbu aizstāvēšanai *(nederīgo svītro vadītājs)*

Vadītājs: profesors, Dr.dat. Māris Vītiņš _____27.05.2019.

Recenzents: docents, Dr.dat. Viesturs Vēzis

Darbs iesniegts Datorikas fakultātē 27.05.2019.

Dekāna pilnvarotā persona: vecākā metodiķe Ārija Sproģe _____

Darbs aizstāvēts bakalauru gala pārbaudījuma komisijas sēdē

__.__.2019. prot. Nr. _____

Komisijas sekretārs(-e): _____