LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

UZŅĒMUMA INFORMĀCIJAS SISTĒMAS PIESKAŅOŠANA JAUNAJAI VISPĀRĪGAI DATU AIZSARDZĪBAS REGULAI

MAĢISTRA DARBS

Autore: **Stella Tīda**
Stud. apl. Nr.: st12048
Darba vadītājs: prof., Dr.dat. Māris Vītiņš

RĪGA 2018

Anotācija

Šis darbs ir pētījums par Vispārīgas datu aizsardzības regulas galveniem aspektiem un atšķirībām no iepriekšējās dokumenta versijas, īpaši izceļot jaunu prasību ietekmi uz uzņēmuma informācijas sistēmām.

Darba pamatteksts ir 43 lappuses. Izmantotās literatūras sarakstu veido 18 avoti.

Pētījuma uzdevumi: izveidot ieteikumus/vadlīnijas esošo informācijas sistēmu pārveidošanai vai jaunu sistēmu izstrādei, kas būtu jāievēro programmatūras izstrādātājiem un jāzin informācijas sistēmu pasūtītājiem, rast IT risinājumus ieteikumu/vadlīniju īstenošanai un pielietot tos pilotprojektā.

Darba teorētisko daļu veido izpētes rezultātā rastie secinājumi par Eiropas datu aizsardzības juridisko dokumentu vēsturi, tiek definēts personas datu jēdziens un tas, kādēļ šie dati ir jāaizsargā, tika apskatītas svarīgākās VDAR prasības un, balstoties uz tām, tika piedāvāti risinājumi un vadlīnijas, kas palīdzēs panākt IS atbilstību šīm prasībām.

Darba praktiskā daļā ir dziļāk izpētītas datu aizsardzības prasības, papildinātas esošās vadlīnijas un ieteikumi, un iegūtās zināšanas un rezultāti pielietoti pilotprojekta izstrādē.

Atslēgvārdi: VDAR, datu aizsardzība, vadlīnijas

Abstract

Company's information system compliance with the new General Data Protection Regulation

This work is a study on the main aspects of the General Data Protection Regulation and the differences from the previous version of the document, with a particular emphasis on the impact of new requirements on enterprise information systems.

The work consists of 43 pages. The list of used literature consists of 18 sources.

The research task is to create recommendations / guidelines for the transformation of existing information systems or the development of new systems that should be followed by software developers and inform the customers of information systems, to find IT solutions for the implementation of recommendations / guidelines.

As a result of the research of the theoretical part of the work, a brief overview of the history of European data protection legal documents was developed, the concept of personal data was defined and why these data have to be protected, the important requirements of the VDAR were considered and based on them, solutions and guidelines were proposed that would help to achieve IS compliance with these requirements.

In the practical part, the data protection requirements are studied deeper, the existing guidelines and recommendations are supplemented, and the acquired knowledge and results are used in the development of a pilot project.

Keywords: GDPR, data protection, guidelines

Autoreferāts

Darba tēma ir ļoti aktuāla 2018. gada pavasarī, jo tieši šajā laikā stājas spēkā jaunas datu aizsardzības prasības, kas ir definētas Vispārīgā datu aizsardzības regulā, kas attiecas uz jebkuru uzņēmumu, kas apstrādā personu datus. Analizējot informācijas avotus, tika konstatēts, ka lielākā daļa uzņēmumu nav gatava izmaiņām, daži pat nezina, kādas ir šīs jaunas prasības. Šī darba uzdevums ir izstrādāt vadlīnijas, kas būtu jāievēro programmatūras izstrādātājiem un jāzina pasūtītājiem, lai izstrādātu atbilstošas regulai informācijas sistēmas vai pielāgotu jau esošās.

Galvenais literatūras avots ir pašas regulas teksts, kā arī citi saistīti ar to juridiskie dokumenti - iepriekšējā datu aizsardzības direktīva, fizisko personu datu aizsardzības likums. Tika izmantoti Datu valsts inspekcijas raksti, aptauju statistikas dati, baltās grāmatas u.c. Iedvesma nāca arī no apmeklētajiem semināriem, kur par tēmu uzstajās gan Datu valsts inspekcijas pārstāvji, gan kolēģi no citām organizācijām un valstīm. Papildus tika vērots citu uzņēmumu progress un idejas, kā viņi sagatavojas tam, lai atbilstu VDAR.

Darba gaitā informācija tika apkopota vadlīnijās, kas tika pielietotas, izstrādājot pilotprojektu. Tā kā laiks bija ierobežots, uzsvars tika likts nevis uz biznesa procesiem, bet tām niansēm, kas padara informācijas sistēmu atbilstošu jaunajai datu aizsardzības politikai. Tā kā uzņēmums ir neliels, un biznesa procesi ir vienkārši, nebija nepieciešams realizēt un detalizēti aprakstīt, piemēram, automatizētus lēmumu pieņemšanas procesus, tomēr uz tiem uzņēmumiem, kur tāda funkcionalitāte ir, attiecas papildus regulas prasības.

Izstrādātā programmatūra ir pieejama GitHub platformā, kur ir atrodama arī instalēšanas pamācība. Visu projektu veido 850 000 koda rindas (kopā ar Symfony ietvaru un bibliotēkām), no kurām 8 500 ir autordarbs. Sistēma ir manuāli testēta un tā strādā, tomēr līdz reālai izmantošanai tā prasa papildus pielāgošanu specifiskām uzņēmuma vajadzībām un funkcionalitātes papildināšanai, piemēram, automātiski ģenerējamo rēķinu kosmētiskās izmaiņas un to automatizēts sūtīšanas process. Turpmāk ir plānots paveikt papildus biznesa vajadzību detalizētu noskaidrošanu kopā ar pasūtītāju, pabeigt klientu pārvaldības sistēmas izstrādi un nodot to ekspluatācijā.

Darba rakstiskā daļa ir noformēta atbilstoši Latvijas Universitātes maģistra darbu izstrādes metodiskiem norādījumiem, tekstā ir izmantota latviešu valodā oficiāli pieņemtā nozares terminoloģija un darba izklāsts ir viegli saprotams.

SATURA RĀDĪTĀJS

APZĪMĒJUMU SARAKSTS

Informācijas sistēma (IS) - cilvēku, datu, procesu un informācijas tehnoloģiju kopums, kurš sadarbojas, lai reģistrētu, uzkrātu un apstrādātu informāciju, kura nepieciešama organizācijas atbalstam.

Datu subjekts - indivīds, par kuru ir ierakstīti personas dati.

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

Datu aizsardzība - process, kas atbalsta personas privāto datu drošību un ierobežo šo datu vākšanu un tālāku izplatīšanu personai nelabvēlīgu mērķu īstenošanai.

Pārzinis - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopā ar citām nosaka personas datu apstrādes nolūkus un līdzekļus.

VDAR - Vispārīgā datu aizsardzības regula.

IEVADS

Vairākums mūsdienu iestāžu un uzņēmumu regulāri izmanto personu datus ikdienā, glabājot, apstrādājot un sniedzot tos citām pusēm, un indivīda privātums ir atkarīgs no daudzu datu vācēju godprātības, tomēr 2018. gada 25. maijā stājas spēkā jaunā Vispārīga datu aizsardzības regula (VDAR), kas ir jaunais Eiropas Savienības datu aizsardzības likums, un ietekmēs to, kā notiek šādas informācijas apstrāde un aprite. Jaunās regulas mērķis ir izlīdzināt datu apstrādi Eiropas valstīs un paaugstināt datu aizsardzības līmeni Eiropas savienības pilsoņiem, kā arī dot iespēju personai kontrolēt, kas un kāpēc apstrādā tās datus [1].

Tas nozīmē, ka daudzas jau eksistējošas uzņēmumu, biedrību, valsts iestāžu, vai pat fizisku personu, kas ir datu pārziņi, informācijas sistēmas jāpieskaņo jaunajām prasībām, vispirms identificējot neatbilstības. Daži IT uzņēmumi piedāvā sniegt konsultācijas uzņēmumiem, Datu valsts inspekcija aktīvi gatavo kvalificētus datu aizsardzības speciālistus [2], un tirgū parādās plašs programmatūras klāsts, kas ir radīts speciāli, lai atvieglotu mazajam biznesam IT ekosistēmas pieskaņošanu regulas prasībām, par (ne)lielu samaksu, protams. Taču ārējie pakalpojumu sniedzēji un nopirktā lietojumprogrammatūra nevar simtprocentīgi garantēt uzņēmuma IS pilnīgu atbilstību regulai, tāpēc ir vērts patstāvīgi izvērtēt situāciju un tad rīkoties.

Šis darbs ir pētījums par VDAR galvenajiem aspektiem, īpaši izceļot jauno prasību ietekmi uz uzņēmuma informācijas sistēmām. Darba uzdevums ir apkopot svarīgākos regulas aspektus un izveidot vadlīnijas, kas palīdzētu mazam biznesam pieskaņot savu informācijas sistēmu jaunajām datu aizsardzības prasībām, nevēršoties pie līdzīgu pakalpojumu sniedzējiem.

Darbu veido piecas daļas. Pirmajā daļā ir ietverts īss ieskats Eiropas datu aizsardzības juridisko dokumentu vēsturē. Nākamajā nodaļā tiek definēts personas datu jēdziens un tas, kādēļ dati ir jāaizsargā, tiek sniegts patlaban vērojamās situācijas īss apraksts. Pēc tam tiek apskatītas svarīgākas VDAR prasības un, balstoties uz tām, tiek piedāvāti risinājumi un vadlīnijas, kas palīdzēs panākt IS atbilstību šīm prasībām. Praktiskajā daļā tiek aprakstīta pētījuma laikā izstrādātā informācijas sistēma mazam uzņēmumam, kurā tika pielietotas vadlīnijas VDAR atbilstībai.

1. DOKUMENTU VĒSTURE

Nepieciešamība veidot vienotu datu aizsardzības politiku Eiropā ir definēta jau sen, un pirms jaunās regulas tika izstrādāti dokumenti, kuri ir ietekmējuši mūsdienu datu aizsardzības politiku.

1.1. Padomes ieteikumi attiecībā uz privātās dzīves un personas datu pārrobežu plūsmas aizsardzības

Mēģinājumi sistematizēt personu datu apriti sākās jau 1980. gadā Eiropā, kad Ekonomiskās sadarbības un attīstības organizācija izdeva personu datu starprobežu plūsmu aizsardzības rekomendācijas, kas saturēja septiņus galvenos principus [3]:

- Datu subjektam jābūt informētam par to, ka tā dati tiek vākti;
- Datiem jābūt izmantotiem tikai noteiktam mērķim, un nekam citam;
- Dati nevar būt atklāti bez datu subjekta piekrišanas;
- Savāktie dati jāglabā droši, tie jāpasargā no potenciāliem apdraudējumiem;
- Datu subjektam jābūt informētam par to, kurš vāc viņa datus;
- Datu subjektam jābūt piekļuvei neprecīzo datu korekcijai;
- Datu subjektam jābūt pieejai metodei, kas nodrošinātu datu vācēju atbildību par iepriekš minēto principu neievērošanu.

Neskatoties uz to, ka šīs vadlīnijas bija nesaistošas (dažādās Eiropas valstīs datu aizsardzības likumi joprojām krietni atšķiras, bet ASV šāda aizsaradzība netika pielietota) tās tomēr tika iekļautas Datu aizsardzības direktīvā.

1.2. Direktīva 95/46/EC

Datu aizsardzības direktīva jeb Direktīva 95/46/EC tika pieņemta 1995. gada 24. oktobrī Eiropas savienībā [4]. Tā tika pieņemta laikā, kad internets vēl bija tā attīstības sākuma stadijā un direktīva attiecās galvenokārt uz ļoti lielām valsts informācijas sistēmām, vai uz papīra kartotēkām. Dokumenta mērķis bija aizsargāt fizisku personu pamattiesības un brīvības, un viņu tiesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi.

Direktīva atzīst personu datu vākšanu un apstrādi par likumīgu, tikai, ja tiek izpildīts kaut viens no kritērijiem [5]:

- Datu subjekts devis savu piekrišanu;
- Apstrāde vajadzīga līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei;
- Apstrāde vajadzīga, lai izpildītu uz personas datu apstrādātāju attiecināmas juridiskas saistības;
- Apstrāde vajadzīga, lai aizsargātu datu subjekta būtiskas intereses;
- Apstrāde vajadzīga sabiedrības interesēs realizējama uzdevuma izpildei vai personas datu apstrādātājam vai trešajai personai, kurai dati tiek atklāti, piešķirto oficiālo pilnvaru realizācijai;
- Apstrāde vajadzīga personas datu apstrādātāja vai trešo personu, kurām dati tiek atklāti, likumīgo interešu ievērošanai.

Kopumā direktīva pozitīvi ietekmēja datu apstrādi. Tā paaugstina izpratni par datu drošības nozīmi, tā ietver sevī drošības principus, un ir elastīga, un ir labās prakses paraugmodelis. Direktīvas principi ir noteikuši personas datu juridisko standartu. Tomēr ir arī svarīgi saprast, ka direktīva tika uzrakstīta laikā, kad datu apstrādē bija iekļautas reģistrācijas sistēmas un lieldatori. Riskus, kas saistīti ar šādu modeli, varētu viegli pārvaldīt, nosakot ar katru funkciju saistītās saistības un procedūras. Tās galvenais mērķis bija saskaņot esošos noteikumus, lai aizsargātu datu subjekta tiesības uz informācijas konfidencialitāti un izveidot vienotu Eiropas tirgu personas datu brīvai apritei, nevis radīt tiesisku regulējumu, kas varētu tikt galā ar nākotnes datu apstrādes un konfidencialitātes problēmām [6].

1.3. Vispārīgā datu aizsardzības regula

Mūsdienu kultūras paradigumu raksturo tīklā izveidota sabiedrība, kurā personas datus nepārtraukti savāc, bagātina, groza, apmainās ar tiem un izmanto tos atkārtoti. Šai jaunajai sociālajai videi ir vajadzīgi labi pielāgoti datu aizsardzības noteikumi, lai novērstu daudz lielākus ļaunprātīgas izmantošanas riskus. Tāpēc 2014. gadā Eiropas parlaments pieņēma jaunu Vispārīgo datu aizsardzības regulu, par to sēdē nobalsoja 621 deputāti, pret nobalsoja 10, un 22 atturējās [4].

Regulā ir ietverti noteikumi, kas no uzņēmumiem prasa aizsargāt ES pilsoņu personas datus un privātumu attiecībā uz darījumiem, kas notiek ES dalībvalstīs. VDAR regulē arī personas datu eksportu ārpus ES. Datu aizsardzības principi tika pārņemti gan no 1980. gadā izstrādātajiem dokumentiem, gan no Direktīvas. Par prasību pārkāpšanu tiks piemērotas soda sankcijas, kas tiek piemērotas atkarībā no pārkāpuma smaguma.

Regulas galvenie personas datu apstrādes principi ir [7]:

- Likumīgums, godprātība un pārredzamība;
- Nolūka ierobežojums;
- Datu minimizēšana;
- Precizitāte;
- Glabāšanas ierobežojums;
- Integritāte un konfidencialitāte;
- Pārskatatbildība.

Atšķirībā no iepriekšējās direktīvas VDAR būtiski paplašina cilvēku tiesības un dod daudz vairāk iespēju kontrolēt to, kas notiek ar viņu datiem, tā dod tiesības pieprasīt no informācijas pārvaldītājiem paskaidrojumus par datu apstrādes mērķiem un procesiem, kā arī iebilst pret datu vākšanu un glabāšanu un pieprasīt datus dzēst. Pašam pārzinim regula uzliek daudz vairāk pienākumu, pirmkārt, pamatot, kāpēc viņam ir vajadzīgi attiecīgie dati, kā arī sniegt pēc datu subjekta pieprasījuma saprotamu informāciju par to, kas un kāpēc tiek darīts ar viņa datiem, un parūpēties par šo datu drošību.

Regula stājas spēkā 2018. gada 25. maijā, tad tā aizstās Direktīvas 95/46/EC darbību.

2. PERSONAS DATU AIZSARDZĪBA

Tā kā regulas mērķis ir personu datu aizsardzība, vispirms jāsaprot, kas ir personas dati, un kāpēc tie jāaizsargā.

2.1. Personas datu definējums

Regulā ir atrodama šāda definīcija:

"Personas dati ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjekts"); 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" [7].

Tātad personas dati iekļauj sevī vārdu, uzvārdu, telefona numuru, e-pasta adresi, pases datus, fizisko adresi, auto reģistrācijas numuru, tiešsaistes identitāti, ģimenes locekļus, ienākumus, piederošos īpašumus, konta numuru, bankas kartes numuru, personas izskatu, internetā izvietotās fotogrāfijas, videomateriālus un citu informāciju.

Īpaša personas datu apakškategorija ir sensitīvie dati, kuri atšķiras no citiem sava privātā un intīmā rakstura dēļ [8]. Šie dati ietver personas rasi vai etnisko izcelsmi, reliģiskos, filozofiskos un politiskos uzskatus, seksuālo orientāciju, dalību arodbiedrībās, tie var attiekties arī uz personas veselību. Tādu datu apstrāde vispārīgā kārtā, izņemot atsevišķus gadījumus, ir aizliegta [7, 9].

2.2. Datu aizsardzības jēga

Personu datus ir svarīgi aizsargāt, jo tā ir daļa no privātās dzīves. Tad, kad personas dati tiek apvienoti, var saprast, kādu dzīvi dzīvo datu subjekts, kādi tam ir paradumi, ģimenes stāvoklis, ko cilvēks pērk vai nepērk u.c. Šo datu atklāšana un analīze var ietekmēt daudzu lēmumu pieņemšanu attiecībā uz cilvēku, piemēram, vai pieņemt viņu darbā utml., tāpēc ir svarīgi aizsargāt cilvēka tiesības uz privātumu un dot viņam iespēju kontrolēt to, kas notiek ar viņa datiem.

Par personu datu aizsardzību ir atbildīgas tās iestādes un uzņēmumi, kuras veic šo datu apstrādi. Par datu noplūdi jeb vispārīgas datu aizsardzības regulas pārkāpumu iestādei piemēro

administratīvu naudas sodu apmērā līdz EUR 20 000 000 vai, ja pārkāpumu izdarījis uzņēmums, līdz 4 % no tā kopējā finanšu gadā gūtā apgrozījuma, pie tam jebkura persona, kurai šī pārkāpuma rezultātā ir nodarīts materiāls vai nemateriāls kaitējums, ir tiesīga no datu pārziņa saņemt kompensāciju [7].

Izņemot tiešos materiālos zaudējumus, kas tiek realizēti soda veidā, uzņēmumam vai iestādei ir risks gūt netiešos zaudējumus, tādus kā kaitējums reputācijai, akciju vērtības pazemināšanas un zaudēti klienti. No datu subjekta puses savukārt ir risks, ka kāds nozags tā identitāti, naudas līdzekļus, vai atklāta informācija var kļūt par pamatu aizspriedumainai attieksmei vai diskriminācijai pret indivīdu.

3. DATU APSTRĀDES UN AIZSARDZĪBAS PRASĪBAS

Šajā nodaļā tiek apkopotas būtiskākās regulas prasības attiecībā uz personu datu apstrādi, kas attiecas uz informācijas sistēmām, darba ietvaros netiks aprakstītas prasības, kas attiecināmas uz reti sastopamiem, neikdienišķiem gadījumiem, kā arī īpašām informācijas sistēmām.

3.1. Datu subjekta piekrišanas nosacījumi

Viens no datu apstrādes likumīguma pamatojumiem ir datu subjekta piekrišana datu apstrādei, kas tiek veikta noteiktiem nolūkiem. Šādā gadījumā pārzinim ir jāspēj parādīt, ka datu subjekts tiešām ir piekritis sniegt savus personas datus [7].

Jebkurā brīdī datu subjektam ir tiesības savu piekrišanu atsaukt. Tas neietekmē to datu apstrādes likumību, kas tika veikta pirms piekrišanas atsaukšanas.

Datu subjektam jābūt informētam par datu izmantošanas piekrišanas atsaukšanas iespēju.

Ja datu subjekts ir bērns kas ir jaunāks par 16 gadiem, tā datu apstrāde ir likumīga tikai tad, ja piekrišanu ir devuši vai apstiprinājuši bērna vecāki vai aizbildņi [7].

3.2. Datu subjektam sniedzamā informācija

Kad dati tiek iegūti no datu subjekta, viņam jāsniedz šāda informācija [7]:

- Pārziņa identitāte un kontaktinformācija;
- Datu aizsardzības speciālista kontaktinformācija, ja tāds ir;
- Datu apstrādes nolūki un juridiskais pamats;
- Personas datu saņēmēji, ja tādi ir;
- Laikposms, cik ilgi personas dati tiks glabāti sistēmā, vai kritēriji, ko izmanto šī laikposma noteikšanai;
- Tas, ka datu subjektam pastāv tiesības pieprasīt pārzinim piekļuvi saviem personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu, vai iebilst pret apstrādi;
- Ja apstrāde tika veikta, balstoties uz datu subjekta piekrišanu, jāinformē par tiesībām jebkurā brīdī atsaukt piekrišanu, neietekmējot datu apstrādes rezultātus, kas iegūti pirms piekrišanas atsaukšanas;
- Datu subjektam ir tiesības iesniegt sūdzību uzraudzības iestādei;

Ja parādas cits nolūks datu apstrādei, par kuru datu subjekts un pārzinis nebija vienojušies, tad pārzinim pirms minētās datu apstrādes jāinformē par to datu subjekts.

3.3. Datu subjekta piekļuves tiesības

Datu subjektam ir tiesības pieprasīt no pārziņa apstiprinājumu par to, vai viņa personas dati tiek vai netiek apstrādāti, ja tiek, tad datu subjektam ir tiesības piekļūt datiem, kā arī saņemt šādu informāciju [7]:

- Apstrādes nolūki;
- Attiecīgo personas datu kategorijas;
- Personas datu saņēmēji, ja tādi ir;
- Laikposms, cik ilgi dati tiks glabāti, vai kritēriji, ko izmanto šī laikposma noteikšanai;
- Informācija par datu avotu, ja dati netika vākti no datu subjekta;
- Jēgpilna informācija par automatizētu lēmumu pieņemšanu un tajā ietverto loģiku, šādas apstrādes nozīmīgumu un sekām attiecībā uz datu subjektu.

Visa šī informācija jāspēj piegādāt datu subjektam plaši izmantotā, pieejamā elektroniskā formā, ja tā nav pieprasīta citādi.

3.4. Personas datu rediģēšana, dzēšana

Datu subjektam ir tiesības pieprasīt neprecīzu datu labošanu vai papildināšanu, kā arī personas datu dzēšanu [7].

Personai ir tiesības “tikt aizmirstai”, ja tiek aktualizēts kaut vai viens no šādiem nosacījumiem:

- Personas datu apstrāde vairs nav nepieciešama;
- Datu subjekts atsauc datu apstrādes piekrišanu;
- Personas dati tiek apstrādāti nelikumīgi;
- Datu apstrādei nav nekāda leģitīma pamata;
- Datu subjekts ir jaunāks par 16 gadiem, un viņa vecāki nav devuši piekrišanu tā datu apstrādei;

Ja personas dati ir publiskoti vai to kopiju apstrādi veic arī citi pārziņi, jāinformē visi apstrādātāji, ka datu subjekts ir pieprasījis datus dzēst, un jāveic nepieciešamie pasākumi, lai pieprasījums tiktu izpildīts.

Atsevišķos gadījumos, piemēram, kad dati tiek vākti un apstrādāti arhivēšanas, statistikas, zinātniskās vai vēsturiskās pētniecības nolūkos, ja datu dzēšana var būtiski traucēt apstrādes mērķu sasniegšanu, dzēšanas pieprasījums var tikt noraidīts.

Datu subjekts var pieprasīt arī ierobežot datu apstrādi, uz laiku vai vispār, ja personas dati ir neprecīzi, to apstrāde ir nelikumīga, pārzinim tie vairs nav vajadzīgi, bet datu subjektam tie ir nepieciešami, vai citā gadījumā. Ja apstrādes ierobežošana tika veikta uz laiku, kamēr pārzinis var pārbaudīt personas datu precizitāti, datu subjekts jāinformē pirms datu apstrādes ierobežojuma atcelšanas.

Pārzinim, ja personas dati tiek izpausti citiem saņēmējiem, labošanas, dzēšanas vai apstrādes ierobežošanas gadījumā jāinformē visi citi saņēmēji. Datu subjekts var pieprasīt arī informāciju par citiem saņēmējiem.

3.5. Datu pārnesamība

Datu subjektam ir tiesības saņemt visus savus personas datus, kas atrodas pārziņa rīcībā, plaši izmantotā mašīnlasāmā formātā, kā arī nosūtīt šos datus tieši no viena pārziņa citam, ja tas ir tehniski iespējams [7].

3.6. Datu aizsardzība pēc noklusējuma

Datu pārziņa pienākums ir efektīvi īstenot tehniskos un organizatoriskos pasākumus datu aizsardzības nodrošināšanai, ņemot vērā apstrādes procesa iespējamos riskus, lai izpildītu regulas prasības un aizsargātu datu subjekta tiesības. Pēc noklusējuma jābūt vāktiem, apstrādātiem un glabātiem tikai tiem datiem, kas ir nepieciešami konkrētajam nolūkam. Bez datu subjekta līdzdalības tā dati nedrīkst būt pieejami nenoteiktam personu skaitam [7].

3.7. Apstrādes darbību reģistrēšana

Ja uzņēmums vai organizācija nodarbina vairāk nekā 250 personas, vai datu apstrāde var radīt risku datu subjektu tiesībām un brīvībai, vai apstrāde nav neregulāra, pārzinim elektroniski jāreģistrē ar datiem veicamās apstrādes darbības, iekļaujot reģistrā šādu informāciju [7]:

- Pārziņa un datu aizsardzības speciālista vārds, uzvārds vai nosaukums un kontaktinformācija;

- Apstrādes nolūki;
- Datu kategoriju apraksts;
- Datu saņēmēji;
- Ja iespējams, datu dzēšanas paredzētie termiņi;

  Ja uzraudzības iestāde pieprasa reģistra datus, tad jānodrošina to pieejamība.

3.8. Apstrādes drošība

Datu pārzinim un apstrādātājam jāveic tehniskie un organizatoriskie pasākumi, lai nodrošinātu datu drošības līmeni atbilstoši riskiem. Tehniski tas varētu iekļaut datu šifrēšanu, apstrādes sistēmu nepārtrauktu konfidencialitāti, integritāti un pieejamību, spēju ātri atjaunot datu pieejamību tehniska negadījuma situācijā, kā arī sistēmas un procesu regulāru testēšanu un novērtēšanu [7].

Jānovērtē drošības līmenis, ņemot vērā tādus riskus kā datu iznīcināšana, nozaudēšana, neatļauta izpaušana vai nesankcionēta piekļuve tiem.

Pārzinim jānodrošina, lai jebkura fiziska persona, kas strādā ar personu datiem, neapstrādā tos bez pārziņa norādījumiem.

3.9. Reaģēšana uz datu aizsardzības pārkāpumu

Ja ir noticis personas datu aizsardzības pārkāpums, kas varētu radīt risku fizisku personu tiesībām un brīvībai, pārzinim jāinformē uzraudzības iestāde un, augsta riska gadījumā, arī datu subjekts [7].

Uzraudzības iestāde jāinformē par pārkāpumu 72 stundu laikā kopš'brīža, kad ir atklāts incidents. Ja tas nav noticis laikā, iesniegumam pievieno kavēšanās iemeslu. Paziņojumā, uzreiz vai pa posmiem, iekļauj šāda informācija:

- Pārkāpuma raksturs, attiecīgas datu kategorijas, aptuvens skarto personas datu ierakstu skaits;
- Datu aizsardzības speciālista vārds, uzvārds un kontaktinformācija, vai kontaktpunkts, kur var iegūt papildus informāciju;
- Pārkāpuma iespējamās sekas;
- Pasākumu apraksts, ko pārzinis veicis, lai novērstu pārkāpumu un tā sekas.

Datu aizsardzības pārkāpumus, to sekas un veiktās koriģējošās darbības pārzinis dokumentē, lai uzraudzības iestāde vajadzības gadījumā varētu to pārbaudīt.

Ja personas dati nebija šifrēti un pārzinis nav veicis nekādus pasākumus, lai novērstu augstu risku personu tiesībām un brīvībām, nekavējoties jāpaziņo datu subjektam par pārkāpumu, ja tas neradīs nesamērīgi lielas pūles. Paziņojumā jāapraksta saprotamajā valodā vismaz kontaktpunkts papildus informācijas iegūšanai, incidenta iespējamās sekas un veikto pārkāpuma novēršanas pasākumu apraksts.

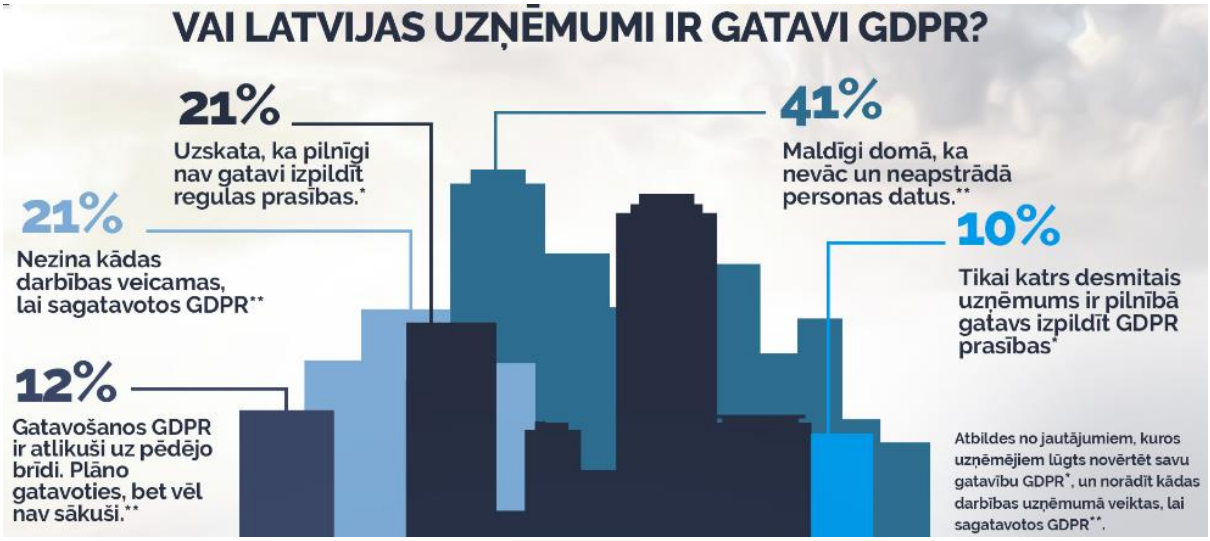
3.10. Datu aizsardzības speciālista iecelšana

Atsevišķos gadījumos, kad apstrādi veic publiska iestāde vai struktūra, vai apstrādātājs plašā mērogā regulāri un sistemātiski veic datu subjektu novērošanu, vai plašā mērogā tiek apstrādāti sensitīvi dati vai dati par sodāmību un pārkāpumiem, pārzinim un apstrādātājam jāieceļ datu aizsardzības speciālists, kam ir šādi uzdevumi [7]:

- Informēt un konsultēt datu aizsardzības jautājumos pārzini, apstrādātāju un darbiniekus;
- Uzraudzīt regulas ievērošanu un uzņēmuma politiku saistībā ar datu aizsardzību;
- Sadarboties ar uzraudzības iestādi un būt par tās kontaktpunktu;

4. INFORMĀCIJAS SISTĒMU PIESKAŅOŠANAS VADLĪNIJAS

Kā liecina publiskotie AS "Norstat Latvija" statistikas dati par VDAR sagatavību Latvijas uzņēmumos (sk. att. 4.1.), tikai 10% no respondentiem no 820 Latvijas uzņēmumiem, kas piedalījās aptaujā, uzskata, ka pilnīgi atbilst regulas prasībām. Aptauja tika veikta 2018. gadā no 19. marta līdz 9. aprīlim, t.i. divus mēnešus pirms regulas spēkā stāšanās datuma [10].



4.1. attēls. **Norstat Latvija apkopoti aptaujas rezultāti par VDAR sagatavotību Latvijā [10]**

Spriežot pēc statistikas datiem, lielākā daļa uzņēmumu (41%) uzskata, ka vispār neapstrādā personu datus, un cita liela daļa (21%) vispār nezina, kādas darbības jāveic, lai sagatavotos VDAR. Uzņēmumi ar mazāku apgrozījumu un mazu darbinieku skaitu ir sliktāk sagatavoti vai vispār nav sagatavoti, salīdzinājumā ar lielākiem uzņēmumiem. Tas varētu liecināt par to, ka galvenokārt trūkst informētības par izmaiņām datu aizsardzības jomā, kā arī varētu ietekmēt finanšu iespēja piesaistīt datu aizsardzības speciālistu.

Datu aizsardzības regulas spēkā stāšanās dienai tuvojoties, tirgū pieaug arī gatavu maksas risinājumu un pakalpojumu skaits, kas atvieglos uzņēmumu informācijas sistēmas pieskaņošanu jaunajām datu aizsardzības prasībām. Protams, tas rada papildus izmaksas, tomēr tiem, kas ir gatavi maksāt, tas varētu būt ērts un drošs veids, kā sakārtot datu apstrādi uzņēmumā.

Uzņēmumiem, kuri nevar vai nevēlas piesaistīt trešās puses un ārpus pakalpojumu sniedzējus, var pieskaņot informācijas sistēmu pašu spēkiem, uzmanīgi izpētot un pielietojot regulas prasības. Lai atvieglotu pielāgošanu, šajā nodaļā tiek piedāvātas vadlīnijas, kas būtu jāievēro informācijas sistēmu izstrādātājiem un pasūtītājiem.

4.1. Risinājumi ar gatavas lietojumprogrammatūras izmantošanu

Programmatūra un mākoņservisi, kuri atbilst regulai, vai palīdz novertēt riskus, ir plaši pieejami. Latvijā tiek īpaši popularizēti divi risinājumi - Microsoft un Snow lietojumprogrammatūra. Viena no tām ir gatavs rīku klāsts darbam ar datiem, otra - rīks, kas palīdz atrast ekosistēmas vājās vietas un riskus.

4.1.1. Microsoft produkcija

Arvien biežāk uzņēmumi un organizācijas datu apstrādi un uzglabāšanu veic, izmantojot progresīvas mākoņservisu tehnoloģijas. Kaut tādā gadījumā dati tieši neatrodas uzņēmuma iekārtās, datu pārziņa pienākums un atbildība ir sekot tam, lai šie dati būtu drošībā.

Microsoft jau sen sniedz mākoņservisu un citu lietojumprogrammatūru pakalpojumus un cenšas izveidot lietotājiem ērtu ekosistēmu, kas atbilst VDAR prasībām. Microsoft produkcijas principiāla pieeja ietver privātuma, drošības un pārredzamības politiku, tas rada klientu uzticību izvēlētajām digitālajām tehnoloģijām. Piedāvātie mākoņservisi nodrošina personu datu dzēšanu, koriģēšanu, pārnesamību, piekļuves kontroli un apstrādes apturēšanu, kā arī savlaicīgu drošības atbalstu, kā to prasa regula [11, 12].

Pašlaik Microsoft nodrošina VDAR atbilstību šādai produkcijai:

- Microsoft Azure
- Microsoft Dynamics 365
- Microsoft Office 365
- Microsoft Enterprise Mobility + Security
- Microsoft SQL Server/Azure SQL Database
- Microsoft Windows 10 un Windows Server 2016

4.1.2. SNOW lietojumprogrammatūra

Zviedru uzņēmums Snow piedāvā VDAR riska novērtējuma programmatūru. Tā atklāj un analizē visas ierīces, kas atrodas īpašumā, atrod starp tām tādas, kas ir nepietiekami aizsargātas, piemēram, vājas šifrēšanas vai antivīrusa programmatūras dēļ. Vāc datus par to, kas, uz kuras mašīnas, un kādu programmatūru ir lietojis. Izceļ lietotnes, kurās ir personu datu zaudēšanas risks. Nepārtraukti kontrolē izmaiņas ekosistēmā un paziņo aizdomīgajam par darbību vai risku tā parādīšanās gadījumā [13].

4.2. Datu aizsardzības speciālista pakalpojumi

Personas datu aizsardzības speciālistu var piesaistīt, pat ja tā nav obligāta prasība, kas atbilst regulas 37. pantam. Šai personai jābūt datu aizsardzības speciālista kvalifikācijai, kuru Latvijā piešķir Datu valsts inspekcija pēc veiksmīgas apmācības kursa apgūšanas un kvalifikācijas pārbaudes sekmīgas nokārtošanas [14].

Datu aizsardzības speciālistu var būt kā uzņēmuma darbinieks, tā arī var sniegt pakalpojumus, pamatojoties uz līguma saistībam. Viņš konsultē datu aizsardzības jautājumos, uzņemas atbildību par datu apstrādes atbilstību regulai un nodrošina datu aizsardzības prasību ievērošanu [7].

4.3. Informācijas sistēmu izstrādes vai pieskaņošanas vadlīnijas

Mazam uzņēmumam, kurš nerada lielus riskus datu subjektu tiesībām un brīvībām to datu apstrādes dēļ, nav nepieciešams meklēt ārējos pakalpojumus un pirkt risku novērtējumu programmatūru, jo panākt uzņēmuma informācijas sistēmas atbilstību VDAR prasībām var patstāvīgi.

4.3.1. Darbinieku un partneru informēšana un apmācība

Pirmkārt, uzņēmuma darbiniekiem un sadarbības partneriem, datu saņēmējiem un citiem apstrādātājiem, ja tādi ir, jābūt zināmam, ka personu datu apstrāde turpmāk notiks pēc VDAR prasībām.

Visiem uzņēmuma darbiniekiem jābūt zināmai viņu lomai un atbildībai drošības politikas sistēmā. Ja nepieciešams, uzņēmumā varētu organizēt lekcijas darbiniekiem, kur īsi un saturīgi tiek aktualizētas jaunās prasības datu drošības jomā, un ar tām saistītās izmaiņas uzņēmuma un personāla darba organizācijā. Jāapmāca darbinieki atpazīt tādus draudus kā "pikšķerēšanas" e-pasta ziņojumi u.c. un jāpaskaidro rīcības, kas nekavējoties jāveic drošības pārkāpuma gadījumā, lai pēc iespējas ātrāk varētu apdraudējumu novērst, t. sk. sistēmas lietotāju paroles maiņa, paziņošana datu drošības speciālistam vai citai atbildīgai amatpersonai, kā arī iespējamo draudu seku novēršana [7, 15, 17].

Atšķirībā no saviem darbiniekiem, uzņēmums nevar ietekmēt savu partneru vai citu datu saņēmēju godprātīgu VDAR prasību izpildi, un, ja rodas šaubas par to datu aizsardzības politiku, ir jāizmanto radikāli risinājumi - vai nu vispār jāatsakās no tādas sadarbības, vai

jāapturē sadarbība, kamēr situācija mainīsies, abos gadījumos jāziņo uzraudzības iestādei, kas Latvijā ir Datu valsts inspekcija, par regulas pārkāpšanu [7].

4.3.2. Personu datu apstrādes audits

Viens no svarīgākajiem soļiem ir identificēt, kādu personas datu glabāšana un apstrāde notiek uzņēmuma informācijas sistēmām un vai visi šie dati tiešām ir nepieciešami mērķu sasniegšanai.

Ja rodas šaubas par to, kā ir formulēts kādas informācijas vākšanas mērķis, tad visticamāk no šo datu apstrādes ir jāatsakās. Gadījumā, ja tiek identificēti sensitīvi dati, ja uzņēmuma pamatdarbība nav zinātniskā vai vēsturiskā pētniecība vai citi gadījumi, kas ir minēti regulas 9. un 10. pantā, no šo datu apstrādes un glabašanas obligāti jāatsakās.

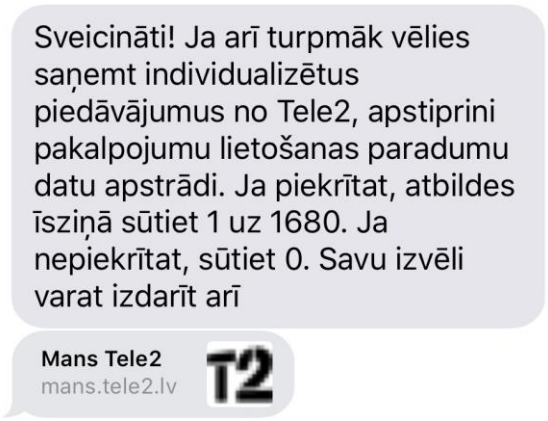
4.3.3. Personu datu vākšanas kārtība

Viena no svarīgākajām lietām vācot personas datus bez citiem juridiskiem pamatiem, ir datu subjekta piekrišana to apstrādei, kā arī informācijas sniegšana par personas tiesībām un cita informācija, kas ir minēta regulas 13. pantā. Tātad jebkurā formā, ko ar saviem personas datiem aizpilda datu subjekts, jābūt izvēles rūtiņai, kas apliecinās, ka lietotājs ir piekritis iesniegt savus datus apstrādei, kā arī jābūt saprotamajā valodā, redzamā vietā izvietotai īsai un saturīgai informācijai par to, kur tieši nonāks iesniegtie dati, ir jābūt informācijai par pārziņa identitāti un kontktinformācijai, kādam mērķim dati tiks apstrādāti, datu aizsardzības specālista kontaktinformācijai, ja tāda ir, un nepieciešamības gadījumā var būt norādīta papildus informācija par datu subjekta tiesībām, datu glabāšanas laikaposmu u.c.

Ja pārziņa rīcībā esošiem personas datiem, kas tika vākti pirms VDAR spēkā stāšanās datuma, nav regulas principiem atbilstošas pierādāmas datu subjekta piekrišanas un pārzinis joprojām grib turpināt šo datu glabāšanu un apstrādi, tad tam būtu jāsaņem datu subjektu piekrišana no jauna, piemēram, nosūtot klientiem e-pastu, kurā tiks paskaidroti apstrādes nolūki, un lūgums sniegt noteikta formāta piekrišanu [17].

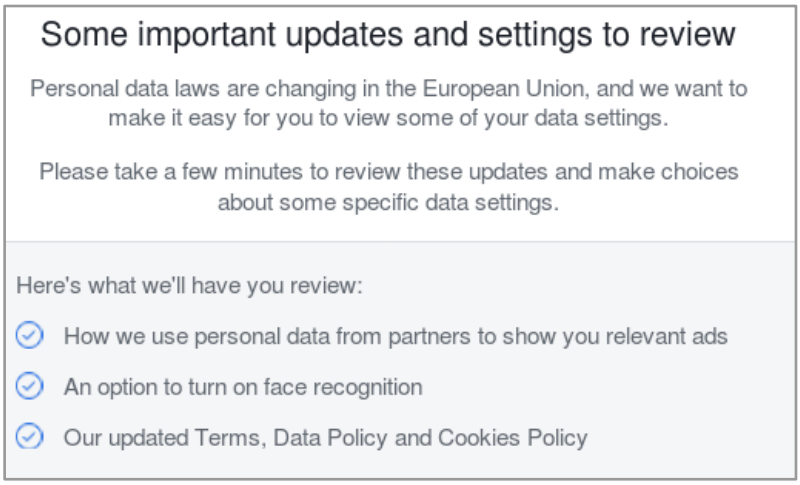
Daži Latvijas uzņēmumi, tādi kā Tele2 piedāvā izvēlēties personu datu apstrādes piekrišanu vai apturēšanu noteiktam mērķim gan lietotāju konta iestatījumos savā mājaslapā, gan īsziņas veidā (sk. att. 4.2.).

Veikalu lojalitātes programmu dalībniekiem arī lūdz iesniegt savu piekrišanu datu apstrādei, piemēram, Mans Rimi kartes īpašniekiem, kur izmaiņas ietekmēja apstrādājamos datus - turpmāk apstrādei netiks lietoti klientu uzvārdi.



4.2. attēls. **Tele2 klientu piekrišana datu vākšanai un datu apstrādei**

Rimi mājaslapā ir ievietots labs piemērs ar paskaidrojumiem saprotamā valodā par atjaunotu programmas privātuma politiku: kādi dati un kādiem mērķiem tiek apstrādāti, kā arī cita informācija, ko nosaka regula datu subjektu informēšanai - glabāšanas ilgums, datu subjektu tiesības, datu aizsardzības speciālista kontaktinformācija u.c. Iesniegt vai atsaukt datu apstrādes piekrišanu ir iespējams gan elektroniski, gan klātienē Rimi tirdzniecības vietās. Līdzīgs rūpīgi izstrādās privātuma politikas dokuments ir pieejams www.barbora.lv interneta veikala tīmekļa vietnē.



4.3. Attēls. **Facebook paziņojums par atjaunotu datu apstrādes politiku**

Sociālie tīkli, piemēram, Facebook, LinkedIn, Instagram un daudzi citi servisi un pakalpojumu sniedzēji, tādi kā Atlassian arī aktīvi informē lietotājus par izmaiņām un pieprasa

piekrišanu datu apstrādes politikai (sk. att. 4.3.). Tomēr regula nosaka to, ka datu subjektam jābūt informētam par to, kam tieši viņš dod piekrišanu.

Gadījumā ar gariem tekstiem rodas šaubas, ka viss dokuments tiks izlasīts, tāpēc būtu efektīvāk pēc iespējas īsāk aprakstīt piekrišanas būtību tieši blakus izvēles rūtiņai, ja šādi notiek piekrišanas apkopojums, bet detalizētu un padziļinātu privātuma politikas dokumentu izvietot citā, visiem interesentiem brīvi pieejamā vietā, vai izsniegt to pēc pieprasījuma - tas nav pretrunā ar regulu.

4.3.4. Gatavība manipulācijām ar datiem

Datu subjekts var pieprasīt manipulācijas ar datiem, kurām sistēmai jābūt gatavai: piekļuve datiem un to kopijas izsniegšana vai pārnešana; visas informācijas par datu apstrādi sniegšana, t. sk. apstrādes nolūki, datu saņēmēji, laikposms, cik ilgi tie tiks glabāti, u.c.; datu labošana; datu dzēšana; datu apstrādes apturēšana; komerciālo sūtījumu aizliegšana.

Būtu ērti, ja visa šī funkcionalitāte būtu implementēta jau iepriekš, it īpaši, ja uzņēmumam nav pastāvīga lietojumprogrammatūras izstrādātāja vai cilvēka, kas varētu piekļūt datubāzei un izpildīt vaicājumus un izmaiņas bez kavēšanās.

Datu dzēšanas pieprasījuma gadījumā jāpādomā par to, kā nesabojāt, piemēram, finanšu atskaišu rezultātus, t.i. dzēst vai anonimizēt tikai personas datus, atstājot pārējo informāciju ierakstā par darījumu, piemēram, darījuma datumu, peļņu, produkta vai pakalpojuma identifikatoru u.c.

Ja dati tiek izpausti arī citiem pārziņiem, to informēšana par datu subjekta pieprasījumu apstrādes statusa maiņai vai datu dzēšanai arī var tikt automatizēta sistēmas lietotāju ērtībai.

4.3.5. Datu glabāšanas ilgums

Datus nedrīkst glabāt neierobežotu laiku, tas nozīmē, ka tad, kad darījums ir noticis, jāizvērtē, kādi dati un cik ilgi pārzinim joprojām ir nepieciešami. Šie dati var būt noderīgi strīdu risināšanā starp pusēm, piemēram, ja ir šaubas par noteikta pakalpojuma vai preces sniegšanas fakta esamību, tomēr pēc noteikta termiņa, piemēram, gada, personas datiem jabūt dzēstiem.

Ja uzņēmumam ir nepieciešama darījumu statistika, pārzinim ir jāizvērtē, vai ir vajadzīgi reāli personas dati. Piemēram, ja tiek analizēti darījumi konkrētā laika periodā, vai ir svarīgi klientu vārdi, uzvārdi un kontaktinformācija, vai tomēr ir svarīgs klientu skaits. Šajā gadījumā saprātīgāk būtu izmantot anonimizētus datus, kas vairs netiek uzskatīti par personas

datiem, un regula uz tiem neattiecas. Tas arī krietni samazinātu draudas un sekas informācijas sistēmas uzlaušanas un datu noplūdes gadījumā.

4.3.6. Piekļuves kontrole

Personas dati nedrīkst būt pieejami nenoteiktam fizisku personu skaitam, tas nozīmē, ka informācijas sitēmā jābūt piekļuves kontroles mehānismam, katram ietotājam piešķirot savus atšķirīgus autentifikācijas līdzekļus - vismaz lietotaja vārdu un paroli, atsevišķos gadījumos - sertifikātus, kodu kalkulatorus vai citus līdzekļus [15]. Piekļuvei personu datiem jābūt tikai tiem darbiniekiem, kuriem tas ir tiešām nepieciešams. No visiem pārējiem lietotājiem personu datiem jābūt slēptiem.

Lietotāja konti un autentifikācijas līdzekļi nekavējoties jābloķē pēc darba attiecību izbeigšanas.

4.3.7. Datu drošība

Viena no svarīgākajām prasībām ir personu datu glabāšanas un apstrādes vairāklīmeņu drošība - gan fiziskā, gan tehnoloģiskā.

Fiziskā līmeņa drošība nozīmē datortehnikas un iekārtu, kur glabājas personu dati, drošība. Kā arī tas, vai ir piekļuve informācijas sistēmai, vai tā ir vai nav pieejama nepiedrošām personām. Datiem šajās iekārtās jābūt aizsargātiem un šifrētiem. Serveriem jābūt izvietotiem atsevišķās telpās ar pastiprinātu aizsardzību, bet rezerves kopiju iekārtas nedrīkst būt brīvi pieejamas [15]. Darbiniekiem, atstājot savu darba vietu, jābeidz visas lietotāja sesijas un jābloķē dators.

Lietotāju datoriem jābūt drošiem pret datorvīrusiem un ārēju ielaušanos, ko var nodrošināt ar regulāri atjauninājamu drošības programmatūras un pareizi konfigurēta ugunsmūra palīdzību.

Ja dati tiek apstrādāti tīmekļa lietojumprogrammatūrā, būtu jānodrošina aizsardzība pret aktuālākajiem un izplatītākajiem uzlaušanas paņēmieniem, kas ir iekļauti Open Web Application Security Project publicētos datos, tajā skaitā skriptu un datubāzes vaicājumu injekcijas, pilnvarošanas mehānisma uzlaušana ar rupjā spēka metodi vai ar vāja paroles atjaunošanas mehānisma izmantošanu u.c.

Lai nepieļautu visizplatītākos uzlaušanas paņēmienus, jānodrošina kvalitatīva ieejas datu pārbaude un simbolu modificēšana (angļ. escaping), jāizveido drošs pieteikšanās mehānisms, pieprasot daudzmaz sarežģītu paroļu veidošanu, jāizmanto drošs jaucējalgoritms

paroļu glabāšanai, ja lietotājs ilgu laiku nav aktīvs lietotnē, tā sesija jābeidz, nedrīkst izpaust tehnisko informāciju kļūdu paziņojumos lietotājiem, kā arī jāreģistrē sistēmas darbības notikumi žurnālā, kurš pēc vajadzības automātiski var ģenerēt un sūtīt paziņojumus atbildīgām amatpersonām par sistēmas darbības traucējumiem vai aizdomīgām darbībām [16].

5. UZŅĒMUMA INFORMĀCIJAS SISTĒMAS IZVEIDE

Šī pētījuma ietvaros tiek veidota informācijas sistēma pasūtītājam, kas ir logu, durvju, žalūziju un metālisko vārtu dažu ražotāju oficiālais dīleris un uzstādīšanas uzņēmums Latvijā. Uzņēmums pārsvarā apkalpo Latvijas iedzīvotājus un vāc personu datus, t.i. Eiropas Savienības pilsoņu datus, tātad, tam jāatbilst VDAR prasībām.

5.1. Pašreizējā situācija

Pašlaik uzņēmumam nav ne vienotās elektroniskās informācijas sistēmas, ne tīmekļa vietnes vizītkartes. Darbinieki izmanto produkcijas ražotāju skicēšanas lietojumprogrammas logu/durvju ieskicēšanai, glabājot attēlus un shēmas nesistematizēti uzņēmuma datorā. Komunikācija ar klientiem pārsvarā notiek klātienē, uzņēmuma tirdzniecības vietās. Klientu dati tiek vākti un glabāti papīra formātā, kā arī rēķini tiek izsniegti drukātā versijā. Uzņēmums izmanto ārpus grāmatvedības firmas pakalpojumus, iesniedzot tai papīra čekus.

Lai attīstītu infrastruktūru un piesaistītu vairāk klientu, uzņēmumam tiek veidota tīmekļa vietne vizītkarte un klientu attiecību pārvaldības sistēma. Turpmāk klienti varēs aizpildīt pieteikuma formu tīmekļa vietnē, kuras iesniegšana automātiski izveidos klientu attiecību pārvaldības sistēmā nepieciešamos biznesa objektus, kas padarīs klienta un darbinieka komunikāciju un pasūtījuma izpildes progresu caurskatāmu, ērti lietojamu, pieejamu un drošāku salīdzinājumā ar pašreizējo situāciju.

5.2. Informācijas sistēmas apraksts

Izstrādājamā sistēma sastāv no divām daļām:

- Aizpildītās formas, kur klients ievad savus personas datus un dod savu piekrišanu to apstrādei;
- Klientu attiecību pārvaldības sistēma (CRM).

Informācijas sistēma ir tīmekļa lietojumprogramma, kas ir pieejama caur tīmekļa pārlūkprogrammu.

Programmas pirmkods ir pieejams GitHub: https://github.com/naginny/relock

5.2.1. Tehnoloģijas

Sistēmas izstrādei tika izvēlēta PHP 7 programmēšanas valoda, Symfony 2.8 ietvars, Doctrine objektrelāciju kartēšana, kā arī atvērta koda dizaina šablons, kas kopumā ietaupīja izstrādes laiku, kā arī piedāvāja jau gatavus drošības risinājumus, tādus kā aizsardzība pret vaicājumu un skriptu injekcijām, ugunsmūra iestatījumu konfigurāciju, drošu piekļuves kontroles un autentifikācijas mehānismu, lietotāju sesijas pārvaldību u.c [18].

Objektrelāciju kartēšanas (*ORM*) tehnologijas pareiza izmantošana nodrošina darbu ar objektiem, nevis tieši ar datubāzi. Doctrine sistēmā ir realizēti vairāki vaicajumu slāņi: no zemākā līmeņa *Connection* līdz *DBAL*, un augstākā līmeņa *ORM* vaicājumiem. Tikai augstākā līmeņa saskarnes izmantošana pasargā lietojamprogrammu no vaicājumu injekcijām (sk. att. 5.1), izvaitories no tīra SQL koda.

```
44          // making a list of clients created at a specific period
45          $em = $this->get('doctrine.orm.entity_manager');
46          /** @var Customer[] $customers */
47          $customers = $em->getRepository('AppBundle:Customer')->createQueryBuilder('c')
48              ->where('c.createdAt >= :from')
49              ->andWhere('c.createdAt <= :to')
50              ->setParameter('from', $request->get( key: 'from', date( format: 'Y-m-d')))
51              ->setParameter('to', $request->get( key: 'to', date( format: 'Y-m-d')))
52              ->getQuery()
53              ->getResult();
54
55          return $this->render( view: 'admin/customers/list.html.twig', array(
56              'title' => 'Customers',
57              'current' => 'customers',
58              'customers' => $customers,
59              'from' => $request->get( key: 'from', date( format: 'Y-m-d')),
60              'to' => $request->get( key: 'to', date( format: 'Y-m-d')),
61          ));
```

5.1. attēls. **Vaicājums ar Doctrine Query Builder izmantošanu**

Symfony ietvars piedāvā aizsardzību pret starpvietņu skriptošanu (XSS), izmantojot iepriekš instalēto Twig veidni (izmantošanas piemērs ir redzams 5.1. att.). Pēc noklusējuma Twig šablonu ietvars pārveido visu lietotāja ievadīto informāciju neinterpretējamā kā izpildāmo kodu saturu (escaping) pirms izvades kā HTML kodu.

Izstrādājama informācijas sistēmā būtiska ieejas datu daļa nāk no klientu aizpildes formas, tāpēc svarīgs ir vēl viens drošības risinājums, kas tiek piedāvāts ietvarā.

Form Builder ir klase, kas implementē drošu pieeju, lai risinātu drošības problēmas aizpildīto formu iesniegšanā tīmekļa lietojumprogrammās.

5.2. attēls. **Symfony iebūvēta aizsardzība pret pārrobežu pieprasījumu viltošanu**

Form Builder klase palīdz veidot formas ar ieejas datu pārbaudi servera pusē (sk. att. 5.3.), kas garantē drošību pret klienta puses datu viltošanu pārlūkprogrammas terminālā, kā arī aizsargā no starpvietņu pieprasījumu viltošanu (att. 5.2.), automātiski iestrādājot CSRF token veidlapās, kad tās tiek ģenerētas, izmantojot *Twig* šablonus.

```
127     /**
128      * @return \Symfony\Component\Form\Form|\Symfony\Component\Form\FormInterface
129      * @throws \Exception
130      */
131     private function getForm()
132     {
133         $amountOf = (function($min, $max) {
134             $choices = array();
135             for($i = $min; $i < $max + 1; $i++) {
136                 $choices[] = $i;
137             }
138             return $choices;
139         });
140         return $this->createFormBuilder()
141             ->add( child: 'name',  type: TextType::class, array(
142                 'required' => true,
143                 'constraints' => array(
144                     new Constraints\Length(array('max' => 255))
145                 )
146             ))
147             ->add('surname', TextType::class, array(
148                 'required' => true,
149                 'constraints' => array(
150                     new Constraints\Length(array('max' => 255))
151                 )
152             ))
```

5.3. attēls. **Formas implementācija, izmantojot iebūvētu Symfony Form Builder klasi**

Vēl viena būtiska sistēmas drošības sastāvdaļa ir autentifikācijas mehānisms, lietotāju piekļuves pārvaldība, sesiju pārvaldība un ugunsmūra iestātījumi. Tas viss ir iekļauts Symfony

Security mehānismā, kas ir ērti pielāgojams vajadzībām caur konfigurācijas failu, kur ir iekļauta lietotāju lomu hierarhija un šīm lomām pieejamu procesu baltais saraksts u.c.

5.2.2. Pasūtījuma pieteikuma forma

Aizpildes forma ir domāta klientiem, kas ir nopietni ieinteresēti veikt pasūtījumu, tāpēc tajā tiek prasīti pasūtījuma izpildei nepieciešami personas dati (5.1. tabula), kas iekļauj: vārdu, uzvārdu, kontakttelefonu, e-pasta adresi un fizisko adresi, kā arī cita papildus informācija par nepieciešamo produkcijas veidu un skaitu, mērījumu un produktu uzstādīšanas vēlamo datumu, piezīmes. Formas ekrānattēls ir pieejams 1. pielikumā. Zemāk uz formas ir aprakstīts savācamo datu apstrādes mērķis, glabāsanas ilgums un pieminētas datu subjekta tiesības. Tiek prasīta piekrišana datu apstrādei izvēles rūtiņas veidā, kaut arī datu subjekta piekrišana nav vienīgais likumīgais pamats datu apstrādei, jo dati ir nepieciešami saistībā ar līgumu vai nodomu noslēgt līgumu. Bez šīs izvēlētās rūtiņas dati netiek iesniegti sistēmā.

5.1. tabula

Pieprasīto personu datu kategorijas, apstrādes pamats

Personas datu kategorija	Apstrādes mērķis	Juridiskais pamats	Glabāšanas periods
Vārds	Datu subjekta identificešana, rēķina izrakstīšana, līguma sastādīšana	Līgumsaistības	2 gadi no pēdējā pasūtījuma izpildes brīža (kamēr ir spēkā garantija) vai 1 gads no pēdējā pasūtījuma atcelšanas brīža (jo klients var atgriezties, un iepriekšējā pasūtījuma dati var noderēt jaunam).
Uzvārds	Datu subjekta identificešana, rēķina izrakstīšana, līguma sastādīšana		
Telefons	Datu subjekta identificešana, saziņa		
E-pasta adrese	Datu subjekta identificešana, saziņa, rēķina izsūtīšana		
Fiziskā adrese	Pakalpojumu, produktu nodrošināšana atbilstoši līgumam		

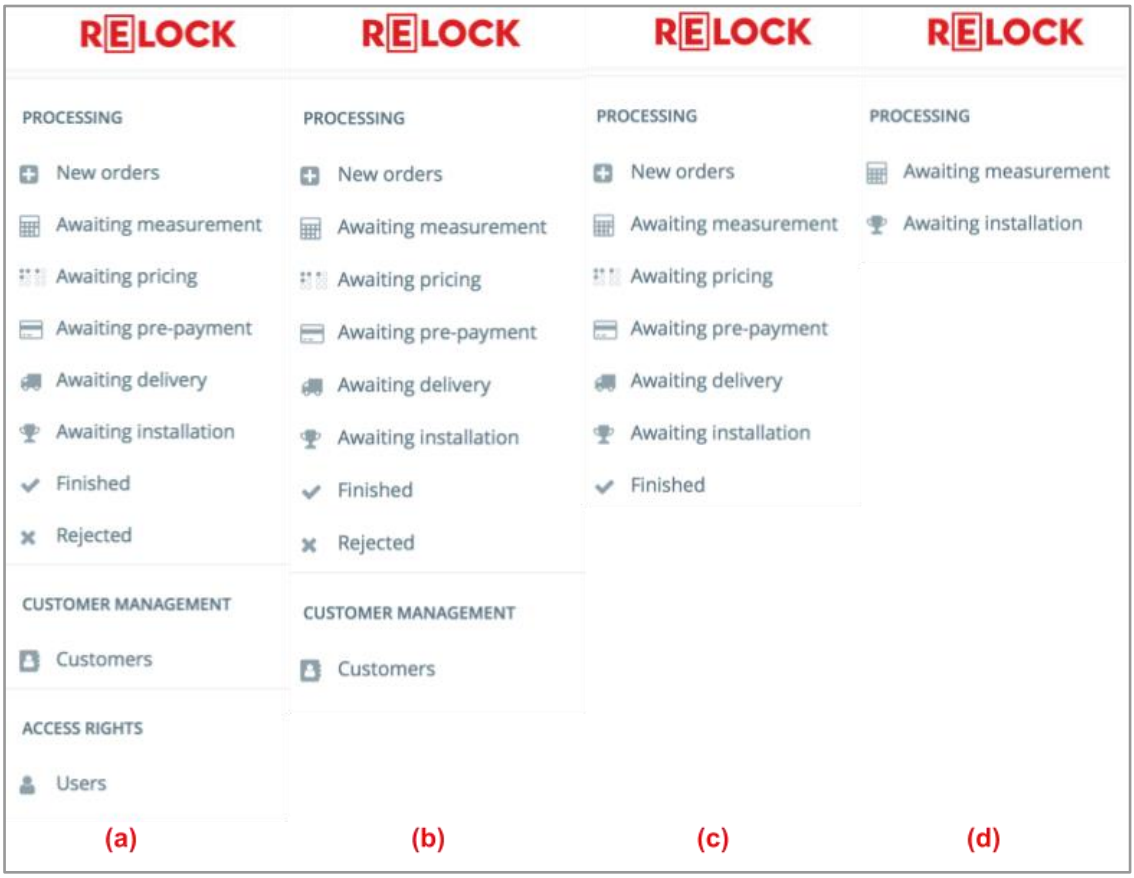
Atšķirībā no iepriekšējā procesa, turpmāk nevarēs prasīt papildus kontaktpersonas telefonu, kas bija normāla prakse uzņēmumā, gadījumā, ja pats klients nevar tikties objektā ar montāžas meistariem, jo tā persona nekādā tiešā veidā nedod savu piekrišanu savas

kontaktinformācijas glabāšanai. Papildus aizpildes formas izveide citai kontaktpersonai šķiet pārmērīga, tāpēc tika pieņemts lēmums no šo datu vākšanas atteikties.

Pēc aizpildītas formas iesniegšanas klientu attiecību pārvaldības sistēmā automātiski tiek izveidots jauns pasūtījums.

5.2.3. Piekļuves kontrole klientu attiecību pārvaldības sistēmā

Kad sistēmā parādas jauns pasūtījums, ar to sāk strādāt uzņēmuma darbinieki. Darbiniekiem sistēmā ir četras lomas: superadministrators, administrators, pārdošanas aģents un uzstādītājs.



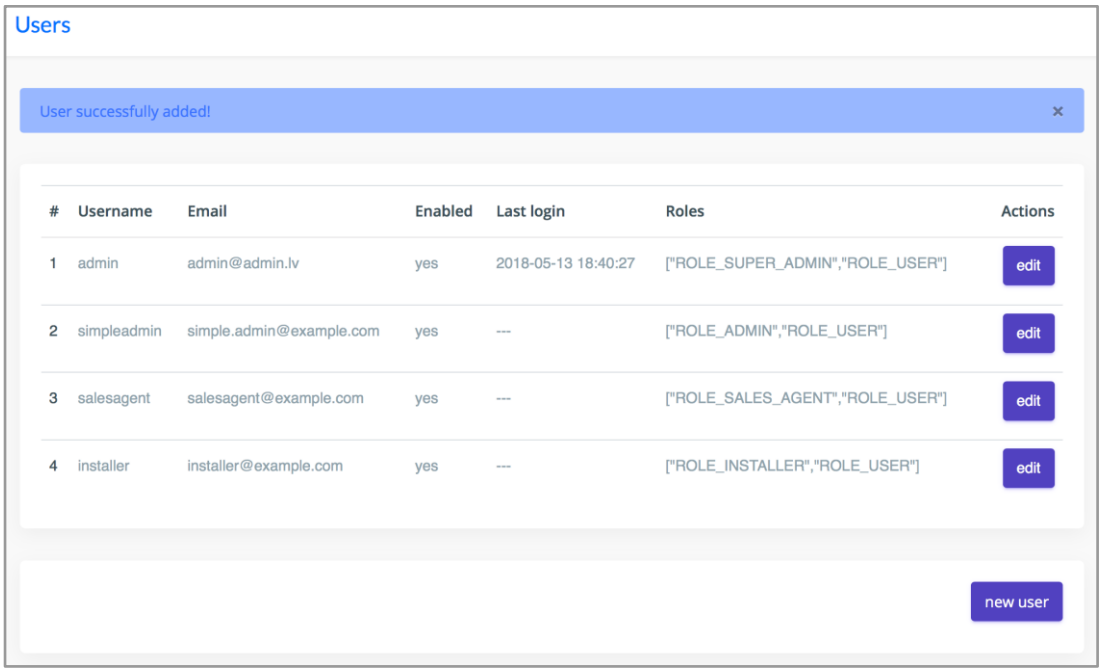
5.4. attēls. **Lietotāju izvēlne atkarībā no lomas:**
(a) superadministrators, (b) administrators, (c) pārdošanas aģents, (d) uzstādītājs.

Katrai lietotāju lomai sistēmā ir savi uzdevumi un ierobežojumi. Klientu attiecību pārvaldības sistēmas izvēlnes atšķirība atkarībā no lietotāja lomas ir redzama attēlā 5.4.

Superadministratoram un administratoram ir visvairāk tiesību, atšķirība ir tikai tāda, ka superadministrators var pārvaldīt citus sistēmas lietotājus - pievienot jaunus lietotājus,

deaktivizēt esošus lietotāju kontus un rediģēt lomas (sk. 5.5. att.). Parastam administratoram šī funkcionalitāte nav pieejama.

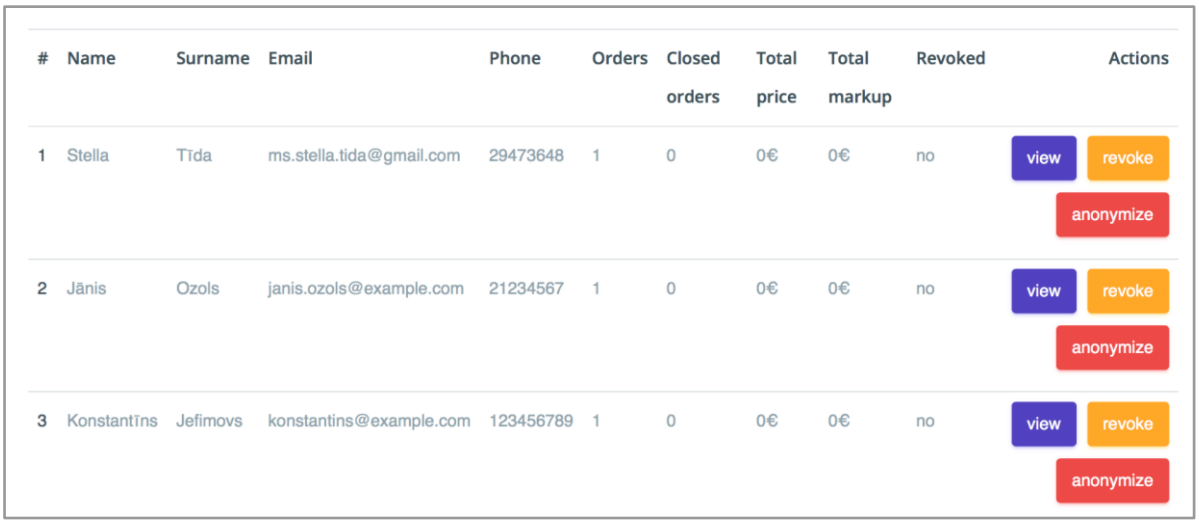
Pārdošanas aģentam ir piekļuve visiem pasūtījumiem un to redigēšanai, bet nav piekļuves visu klientu sarakstam ar iespējām anonimizēt personu datus lietotāju saskarnē vai datubāzē (sk. 5.6. att.).



5.5. attēls. **Lietotāju ierakstu rediģēšanas skats**

Ja no datu subjekta tiek pieprasīta visa par viņu esošā informācija, kas ir datu pārziņa rīcībā, un/vai šo datu rediģēšana vai dzēšana, tad to pieprasījumu pilda administrators vai superadministrators.

Pārdošanas aģenta loma ir pieņemt pasūtījumus, izsekot to progresu, veikt konsultācijas un atbalstu klientiem, un vest pasūtījumus līdz finmāla stadijai.



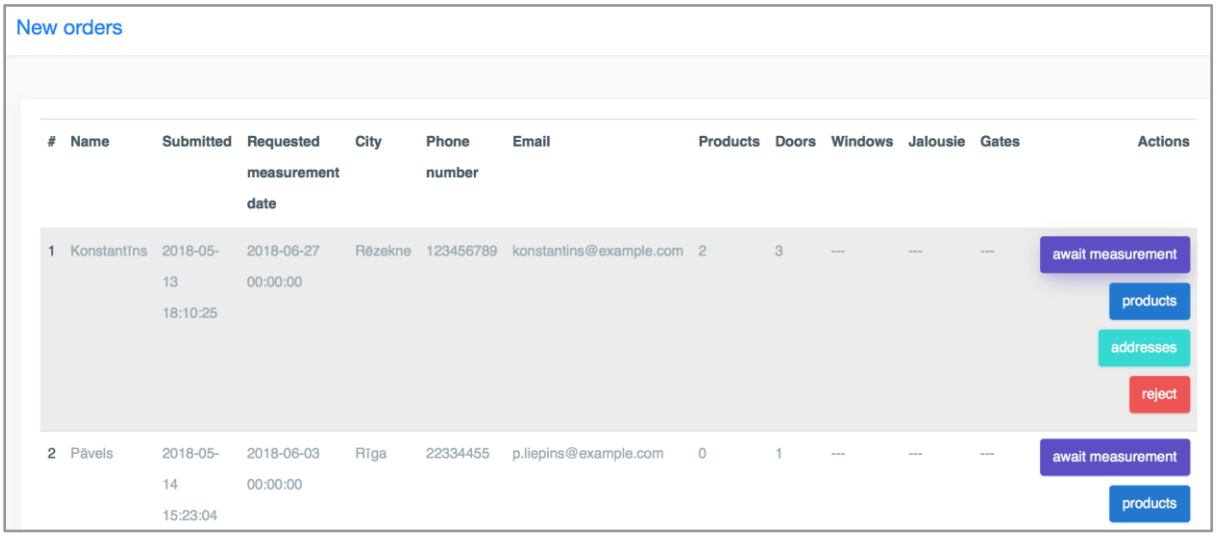
5.6. attēls. **Klientu ierakstu rediģēšanas skats**

Uzstādītājs ir tāds darbinieks, kas veic pasūtījuma izpildei nepieciešamus mērījumus objektā un gatavu produktu uzstādīšanu un montāžu, tāpēc uzstādītājiem ir visierobežotākās tiesības, un tie redz sistēmā tikai pasūtījumus attiecīgās stadijās - tos, kuriem ir nepieciešami mērījumi, vai montāža, kā arī šīs lomas lietotāji neredz klientu e-pastu adreses, jo tas nav nepieciešams viņu darbam.

5.2.4. Biznesa objekti un lietošanas scenārijs

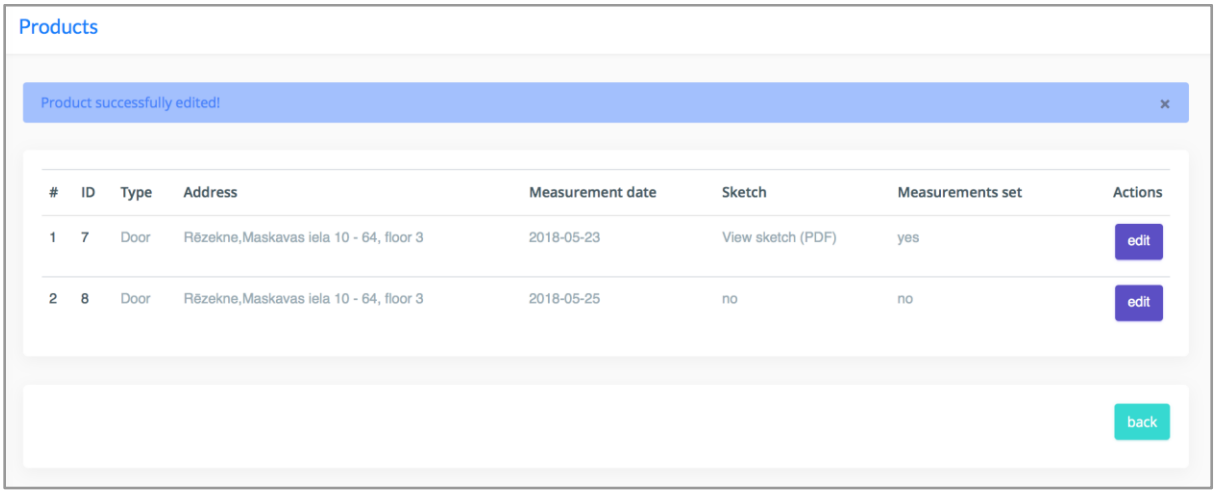
Pēc pasūtījuma pieteikuma formas iesniegšanas klientu attiecību pārvaldības sistēmā automātiski izveidojas trīs objekti: klients, klienta adreses informācija un pasūtījums ar statusu “jauns” (sk. att. 5.7.). Ja sistēmas datubāzē jau eksistē ieraksts ar iesniedzamu e-pasta adresi un telefonu, tad šis klients tiek identificēts kā jau esošais, un pasūtījums tiek saistīts ar eksistējošu klienta ierakstu.

Datubāzes shēmas attēls ir pieejams 2. pielikumā.



5.7. attēls. **Jaunu pasūtījumu skats**

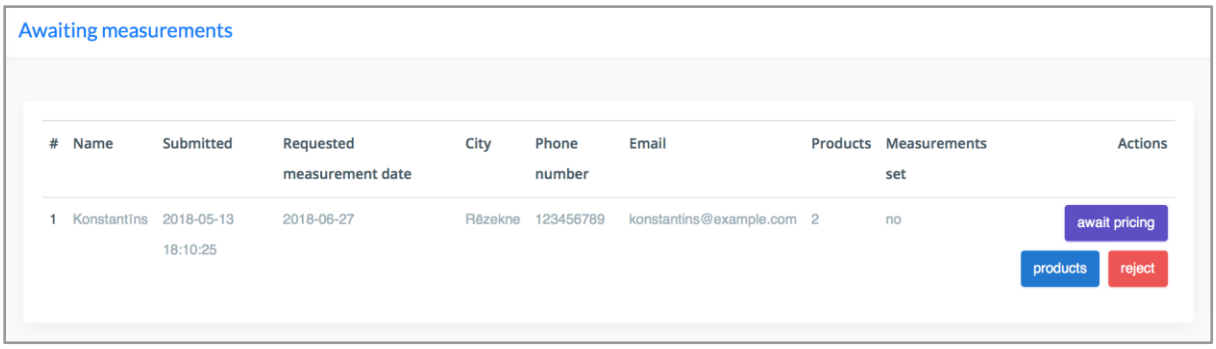
Pēc jauna pasūtījuma pievienošanas, ar klientu sazinās pārdošanas aģents, papildinot pasūtījumu ar jaunu informāciju - vienojas ar klientu par reālu mērījumu datumu, pievieno pasūtījumam konkrēta tipa produktu objektus (attēls 5.8.), ja nepieciešams - pievieno papildus adreses, kas ir saistīti ar produktiem, jo var gadīties, ka vienā pasūtījumā nekustamā īpašuma objekti atrodas dažādās vietās.



5.8. attēls. **Pasūtījuma produktu saraksts**

Pēc nepieciešamās informācijas aizpildīšanas, pasūtījums nonāk nākamajā statusā - "gaida mērījumu" (sk. att. 5.9.).

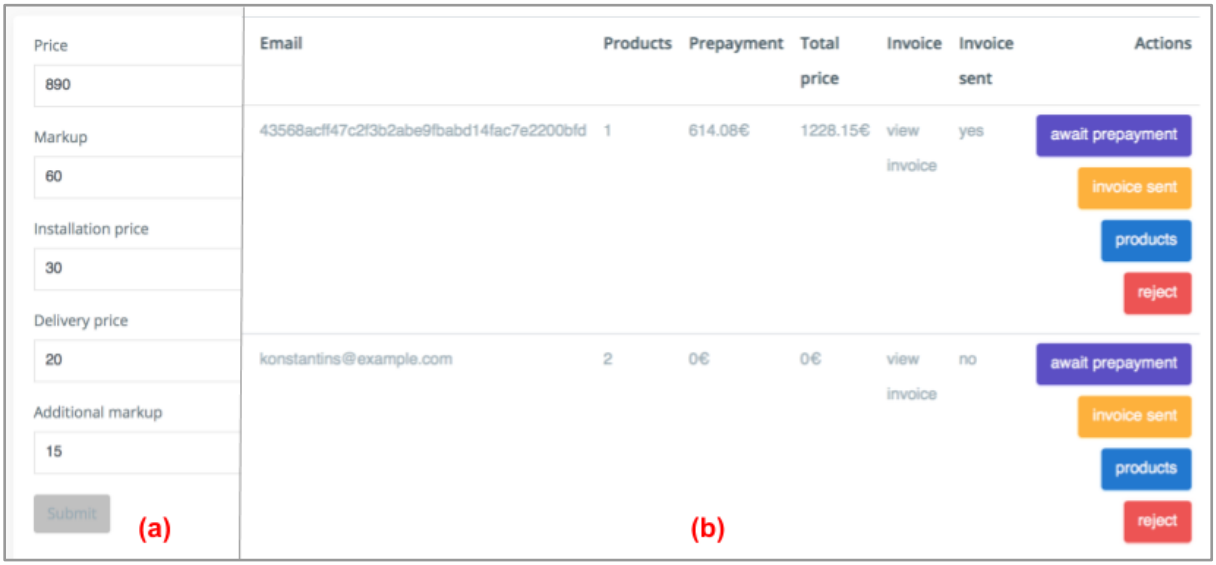
Šajā stadijā pasūtījumam ir visi biznesa objekti, bet ne līdz galam aizpildīti ar informāciju.



5.9. attēls. **Pasūtījumu saraksts ar statusu "Gaida mērījumu"**

Tālāk ar pasūtījumu sāk strādāt uzstādītājs, kurš ievad sistēmā detalizētu informāciju par produktiem - izmērus, izvēlētu ražotāju, modeli un apdares opciju, kā arī augšupielādē produkta skices datni. Ar šiem datiem pasūtījums nonāk nākamā stadijā - "gaida cenas noteikšanu" (sk. att. 5.10.).

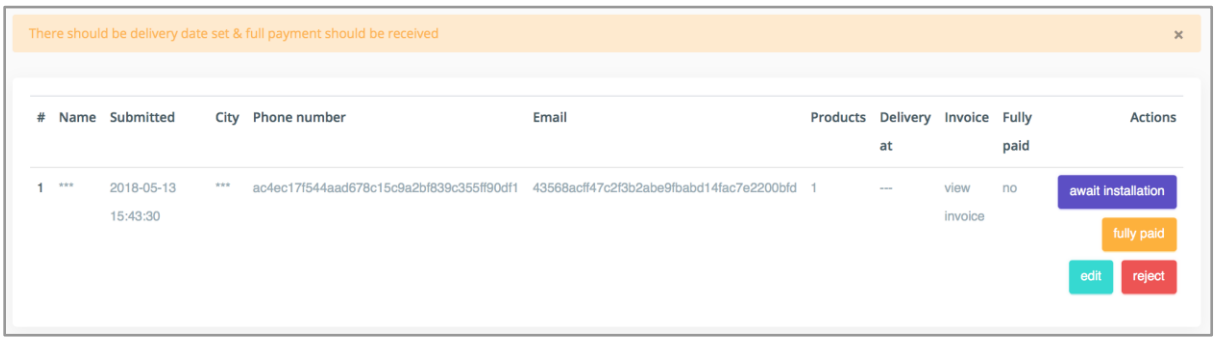
Dažiem ražotājiem ir standarta cenas, dažiem jārēķina cena katram konkrētam produktam atsevišķi.



5.10. attēls. **Produkta cenas rediģēšanas skats (a) un pasūtījumu saraksts "gaida cenas noteikšanu" statusā (b)**

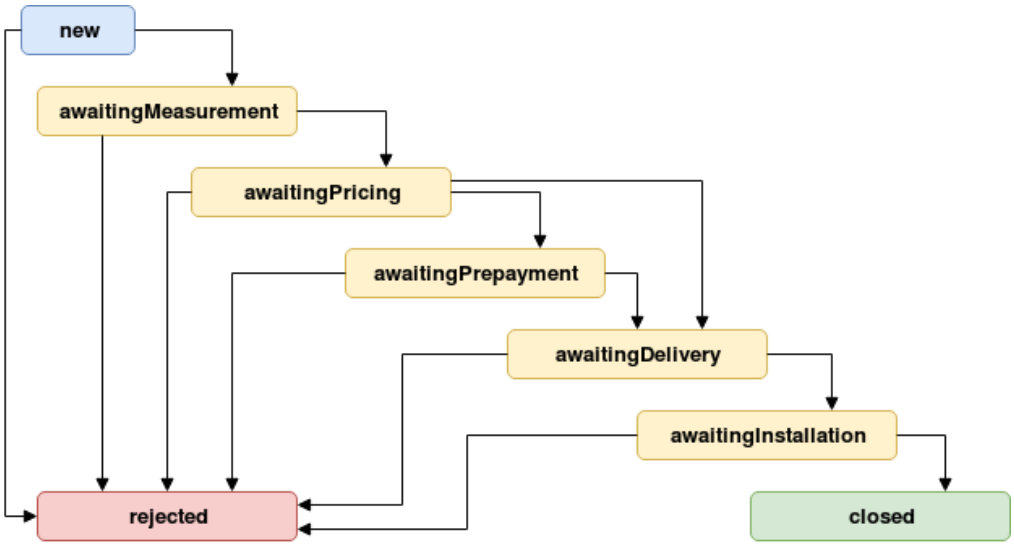
Ja cena ir zināma uzreiz, klients var apmaksāt avansu uzreiz pēc mērījumiem, un šādi iedarbot produktu izgatavošanas procesu, citādā gadījumā process ir nedaudz garāks.

Kad cena ir noteikta un aizpildīta katram produktam, klients ir informēts un piekritis, avanss ir saņemts un attiecīgi atzīmēts pasūtījumā, sākas izgatavošanas process, kas kopā ar piegādi no ražotāja var ilgt no divām nedēļām līdz pusotram mēnesim. Visu šo laiku pasūtījums atrodas "gaida piegādi" statusā (sk. att. 5.11.).



5.11. attēls. **Pasūtījums statusā "gaida piegādi" ar paziņojumu, ka tas nav gatavs pārcelties uz nākamo statusu**

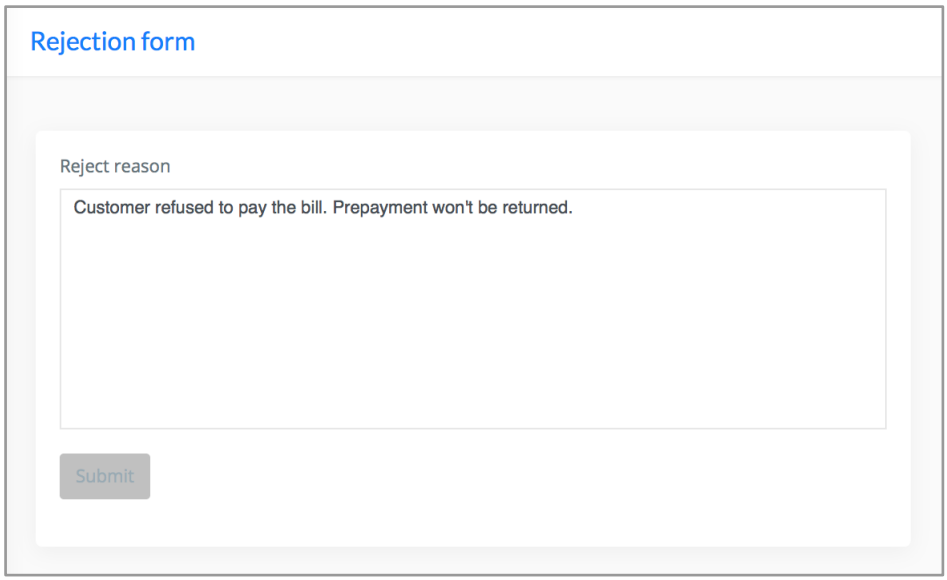
Kad produkts ir veiksmīgi piegādāts, ar klientu sazinās pārdošanas aģents un sarunā montāžas datumu. Šajā laikā pasūtījuma pilnai summai jābūt apmaksātai. Kad montāžas datums ir noteikts un pasūtījums ir atzīmēts kā pilnīgi apmaksāts, to pārcel uz nākamo sarakstu ar statusu "gaida montāžu" un ar to atkal sāk strādāt uzstādītāji.



5.12. attēls. **Pasūtījuma dzīves cikls.**

Pēc visu produktu uzstādīšanas, pasūtījums tiek slēgts. Pasūtījuma statusi un dzīves cikls sistēmā ir redzams attēlā 5.12.

Katrā stadijā, izņemot pēdējo statusu ”slēgts”, pasūtījums var būt atteikts, norādot iemeslu (attēls 5.13.).



5.13. attēls. **Pasūtījuma atteikšanas forma.**

Šādi klientu attiecību pārvaldības sistēma nodrošina darījumu pārvaldību no sākuma līdz beigu stadijai.

5.2.5. Automatizēti procesi

Sistēmā ir divi automatizēti procesi: darbību ierakstīšana notikumu žurnālā un vecu klientu datu anonimizēšana.

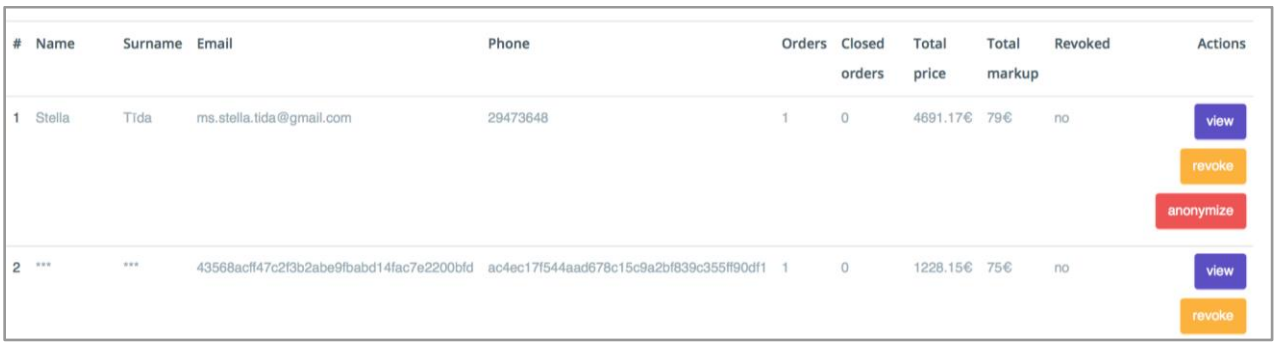
... 1	customer_id	employee_id	action	message	created_at
29	1	1	order changed status to closed	order id: 1	2018-05-13 21:22:36
28	1	1	order product installation changed	order id: 1	2018-05-13 21:22:26
27	1	1	order changed status to awaitingInstallat…	order id: 1	2018-05-13 21:22:05
26	1	1	order payment received	order id: 1	2018-05-13 21:21:55
25	1	1	order product delivery changed	order id: 1	2018-05-13 21:21:48
24	1	1	order changed status to awaitingDelivery	order id: 1	2018-05-13 21:21:22
23	1	1	order changed status to awaitingPrepayment	order id: 1	2018-05-13 21:21:09
22	1	1	order invoice sent	order id: 1	2018-05-13 21:20:38
21	2	1	order product pricing changed	order id: 2, product id: 6	2018-05-13 21:19:41
20	2	1	order changed status to awaitingPricing	order id: 2	2018-05-13 21:17:34

5.14. attēls. **Notikumu žurnāla ieraksti datubāzē**.

Darbības notikumu žurnālā tiek saistītas ar darbinieku un klientu (attēls 5.14.). Lietotāju saskarnē notikumu žurnāla ieraksti tiek attēloti klientu rediģēšanas skatā, kas ir pieejams tikai administratoriem un superadministratoriem.

Žurnāla ieraksti var tikt paplašināti ar izmaiņu detaļām (kādi dati tika mainīti pret kādiem), tomēr jāatceras, ka visa ierakstīta personu informācija jādzēš pēc noteikta perioda vai pēc pieprasījuma, tajā skaitā no šādiem žurnāla ierakstiem.

Klientu datu anonimizēšana notiek divos veidos. Pirmais ir automatizēts *cron* uzdevumu plānotājs, kas reizi dienā meklē datubāzē klientus, kuriem pašlaik nav aktīvu pasūtījumu, un pēdējais izpildītais ir jau divu gadu vecs, vai pēdējais atteiktais ir vienu gadu vecs. Ja klients tomēr ir pieprasījis izdzēst viņu datus no sistēmas agrāk par šo periodu, to ir iespējams izdarīt no klientu pārvaldības skata lietotāju saskarnē, kas ir pieejams administratoriem un superadministratoriem.



5.15. Attēls. **Aktīvs klients (#1) un anonimizēts klienta ieraksts (#2) lietotaju saskarnē.**

Manuāli ir divi veidi, kā rīkoties ar datiem: pirmais - paslēpt datus tikai no lietotāju saskarnes, atstājot tos datubāzē neskartus; otrais - izdzēst visus personas datus no datubāzes, atstājot tikai informāciju par pasūtījumu, pēc kuras nevar identificēt klientu (sk. att. 5.15.). Pirmais variants varētu noderēt gadījumā, ja klients vēlas tikai apturēt datu apstrādi, nevis dzēst pavisam.

5.2.6. Darbības ar klientu ierakstiem

Administratoriem un superadministratoriem ir piekļuve klientu sarakstam, kur var apskatīt visu par klientu savākto informāciju - personas datus, pasūtījumu vēsturi, pasūtītos produktus, produktu detaļas, cenas u.c. No šī ekrāna var paslēpt klienta personas datus no lietotāju saskarnes, atstājot tos datubāzē ar iespēju atgriezt atpakaļ saskarnē vai anonimizēt uz visiem laikiem, t.i. izdzēst no datubāzes.

Taču regulā vēl ir definētas datu subjekta tiesības piekļūt datiem, un tiesības uz datu pārnesamību.

	A	B	C	D	E	F	G	H	
1	Customer information								
2	id	Created at	Name	Surname	Email	Phone	Permission To Use PersonalInfo	Permission Received At	Perr
3	1	2018-05-14 15:33:26	Stella	Tīda	ms.stella.tida@gma	29473648	yes	2018-05-14 15:33:26	
4	Customer addresses								
5	id	City	Street	Floor	Notes				
6	1	Rīga	Klusā iela 18/20 -1009	9	Lūgums nezvanīt agrāk par 12:00				
7	8	Rīga	Klusā iela 18/20 -1009	9	Man jau ir pie Jums pasūtījums, vajag uztaisīt vēl žalūzijas.				
8	Customer orders								
9	Id	Created At	Closed At	Requested Meas	Requested Installat	Requested Door	Requested Window Amount	Requested Jalousie Amo	Req
10	1	2018-05-13 14:46:17	2018-05-13 21:22:36	2018-05-20 0:00:	2018-06-13 0:00:00	0	2	2	
11	8	2018-05-14 15:33:26	---	2018-05-21 0:00:	2018-06-14 0:00:00	0	0	1	
12	Customer products								
13	Id	Measurement	Installation	Material	Manufacturer	Price	VendorCode	Notes	Sket
14	1	2018-05-20 0:00:00	---			1000			
15	2	2018-05-20 0:00:00	---			356			
16	3	2018-05-20 0:00:00	---						

5.16. Attēls. **Informācija par klientu *csv* formātā**

Šajā informācijas sistēmā ir implementēta iespēja lejupielādēt no klientu datu skata visu par viņu savākto informāciju (sk. att. 5.16.), neskaitot notikumu žurnāla ierakstus un uzcenojuma informāciju, jo tas ir komerciāls noslēpums. Dati tiek lejupielādēti *csv* formātā, tātad tie ir gan cilvēkam saprotami, gan mašīnlasami, kas atbilst gan piekļūšanas, gan datu pārnesamības prasībām.

REZULTĀTI

Pētījuma rezultātā tika izveidotas vadlīnijas, kuras ietver būtiskākos jaunās datu aizsardzības politikas aspektus, kas ir: nepārprotama datu subjekta piekrišana datu apstrādei; apstrādājamo datu audits un apstrādes mērķu definēšana; datu subjekta tiesības datu piekļūšanai, rediģēšanai, dzēšanai vai pārnešanai citam datu pārzinim; definēts datu glabāšanas periods; pietiekams drošības līmenis datu apstrādē.

Sastādītās vadlīnijas tika pielietotas pilotprojekta izstrādē, kurš atbilst visiem minētiem nosacījumiem. Klientu pieteikuma formā tiek prasīti tikai pakalpojumu un produktu nodrošināšanai nepieciešami dati, kā arī tiek prasīta datu subjekta piekrišana iesniedzamo datu apstrādei ar īsi un saprotami noformulētu apstrādes mērķi, datu pārziņa identitāte un kontaktinformācija, un informācija par klienta tiesībām iebilst apstrādei. Visi par klientu savāktie dati var tikt lejupielādēti mašīnlasāmā formātā un nodoti datu subjektam vai citam viņa izvēlētam datu pārzinim. Klientu informācija var tikt rediģēta, paslēpta no lietotāju saskarnes bez dzēšanas no datubāzes vai pilnīgi un bezatgrieziniski anonimizēta. Visas darbības informācijas sistemā tiek ierakstītas notikumu žurnalā un ir izsekojamas. Sistēma ir pietiekami aizsargāta pret izplatītākiem uzlaušanas paņēmieniem, kā arī no nesankcionētas piekļuves uzņēmuma vidē, jo ir implementēts drošs piekļuves kontroles mehānisms. Darbinieki redz tikai to informāciju, kura viņiem it nepieciešama viņu darba veikšanai. Produkcijas vidē svarīgākie ieraksti datubāzē, t.i. visi *customer* un *customer_address* tabulu dati tiks šifrēti.

Uzņēmumam šis informācijas sistēmas risinājums ir liels ieguvums, jo pirms tam viņu rīcībā nebija līdzīgu rīku, kas atvieglotu darba procesu pārskatamību, sistematizētu glabāšanu, ērtu pieejamību, kā arī iespēju paplašināt jaunu klientu piesaisti, piedāvājot viņiem ērtu elektroniskās saziņas veidu. Uzņēmuma parstāvji šī pētījuma laikā ieguva jaunu informāciju, jo viņu uzņēmumu var attiecināt uz to riska grupu darbā apskatītajā statistikā [10], kas vismazāk ir informēti par VDAR ieviešanu un tā sekām, kā arī par nepieciešamām izmaiņām, kas būtu jāievieš, lai atbilstu jaunajām prasībām, un ir vismazāk sagatavoti regulas ieviešanai. Šobrīd situācija ir pozitīvi mainījusies - tika veikts datu audits, personāls ir informēts par datu aizsardzības politiku, ir izstrādāta prasībām atbilstoša informācijas sistēma, un sadarbība vēl tiks turpināta, kā arī jau piemeklētie risinājumi tiks pilnveidoti un programmatūra tiks labāk pielāgota uzņēmuma veiksmīgam darbam.

SECINĀJUMI

Analizējot Vispārīgās datu aizsardzības regulas prasības tika skaidrs, ka izmaiņas datu aizsardzības politikā jaunā līmenī dos iespēju izvērtēt tādas vērtības kā uzticība un drošība attiecībā pret informācijas un komunikācijas tehnoloģijām. Regula paaugstinās datu aizsardzības līmeni Eiropas Savienības pilsoņiem, kā arī dos iespēju cilvēkiem kontrolēt daļu no savas privātās dzīves, kas līdz šim bija iespējams, taču ne vienmēr. Pienākumi un principi, kas turpmāk būs jāievēro personu datu pārziņiem, ir priekšrocība arī viņiem pašiem, jo tas palīdzēs "sakārtot" viņu rīcībā esošās informācijas sistēmas, palīdzēs radīt pilnīgāku priekšstatu par sistēmās notiekošajiem procesiem, varbūt atklās iemeslus, kādēļ ir vērts pārveidot un modernizēt novecojušas tehnoloģijas, un, protams, minimizēs risku saskarties ar problēmām, kas ir saistītas ar personu datu noplūdi, uzlaušanu un zagšanu, tādējādi izvairīties no nepatikšanām, tādām kā finanšu sankcijas, reputācijas sabojāšana un klientu uzticības zaudēšana, bet atsevišķos gadījumos pat krimināltiesiskā atbildība.

Šī pētījuma ietvaros tika atrasti risinājumi, kas būtu jāņem vērā informācijas sistēmu izstrādātājiem un būtu jāzina to pasūtītājiem. Iegūtie rezultāti un pilotprojekta izstrādes aprakstītā pieredze var noderēt citu mazo biznesu informācijas sistēmu izstrādē un pielāgošanā, tika noskaidrots, ka sniedzot uzņēmumam pietiekamu informāciju par tēmu, nav sarežģīti ieviest nepieciešamās izmaiņas uzņēmuma privātuma politikā un personu datu apritē.

IZMANTOTĀ LITERATŪRA UN AVOTI

1. *"GDPR Key Changes"*, EU GDPR Portal. Pieejams: http://www.eugdpr.org/

2. *"Datu aizsardzība"*, Datu valsts inspekcija. Pieejams: http://www.dvi.gov.lv/lv/datu-aizsardziba/

3. *"Data Protection Directive"*, Wikipedia, 2018. Pieejams: https://en.wikipedia.org/wiki/Data_Protection_Directive

4. *"The History of the General Data Protection Regulation"*, European Data Protection Supervisor. Pieejams: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

5. *"Eiropas Parlamenta un Padomes Direktīva 95/46/EK"*, Eiropas Parlaments un Eiropas Savienības Padome, 1995. Pieejams: http://www.ic.iem.gov.lv/sites/default/files/EP_direktiva_95_46_EC_personas_aizsardziba_datu_apstrade_24101995.pdf

6. *"Review of the European Data Protection Directive"*, N. Robinson, H. Graux, M. Botterman, L. Valeri, 2009. Pieejams: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf

7. *"Eiropas Parlamenta un Padomes Regula (ES) 2016/679"*, Eiropas Parlaments un Eiropas Savienības Padome, 2016. Pieejams: http://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32016R0679&from=LV

8. *"Kas ir personas dati"*, Cilvēktiesību Gids. Pieejams: http://www.cilvektiesibugids.lv/lv/temas/dati-privatums/kas-ir-datu-aizsardziba/kas-ir-personas-dati

9. *"Fizisko personu datu aizsardzības likums"*, Latvijas Republikas Saeima, 2000. Pieejams: https://likumi.lv/ta/id/4042-fizisko-personu-datu-aizsardzibas-likums#p-434838

10. *“Vai Latvijas uzņēmumi ir gatavi GDPR?”*, A/S Norstat Latvija, 2018. Pieejams: https://squalio.com/wp-content/uploads/2018/04/GDPR_aptauja_uznemumu_gataviba.pdf

11. *“How our products help with GDPR compliance”,* Microsoft. Pieejams: https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/solutions

12. *”Beginning your General Data Protection Regulation (GDPR) Journey”*, white paper, Microsoft, 2017. Pieejams: https://aka.ms/gdprwhitepaper

13. *“Snow GDPR Risk Assessment”*, Snow Software, 2018. Pieejams: https://www.snowsoftware.com/int/products/snow-gdpr-risk-assessment

14. *“Kā iegūt personas datu aizsardzības speciālista kvalifikāciju”*, Datu valsts inspekcija, 2017. Pieejams: http://www.dvi.gov.lv/lv/datu-aizsardziba/ka-klut-par-specialistu/

15. *“Rekomendācija. Personas datu apstrādes drošība”*, Datu valsts inspekcija, 2014. Pieejams: http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Rekomendacija_PDA_drosiba_2014.pdf

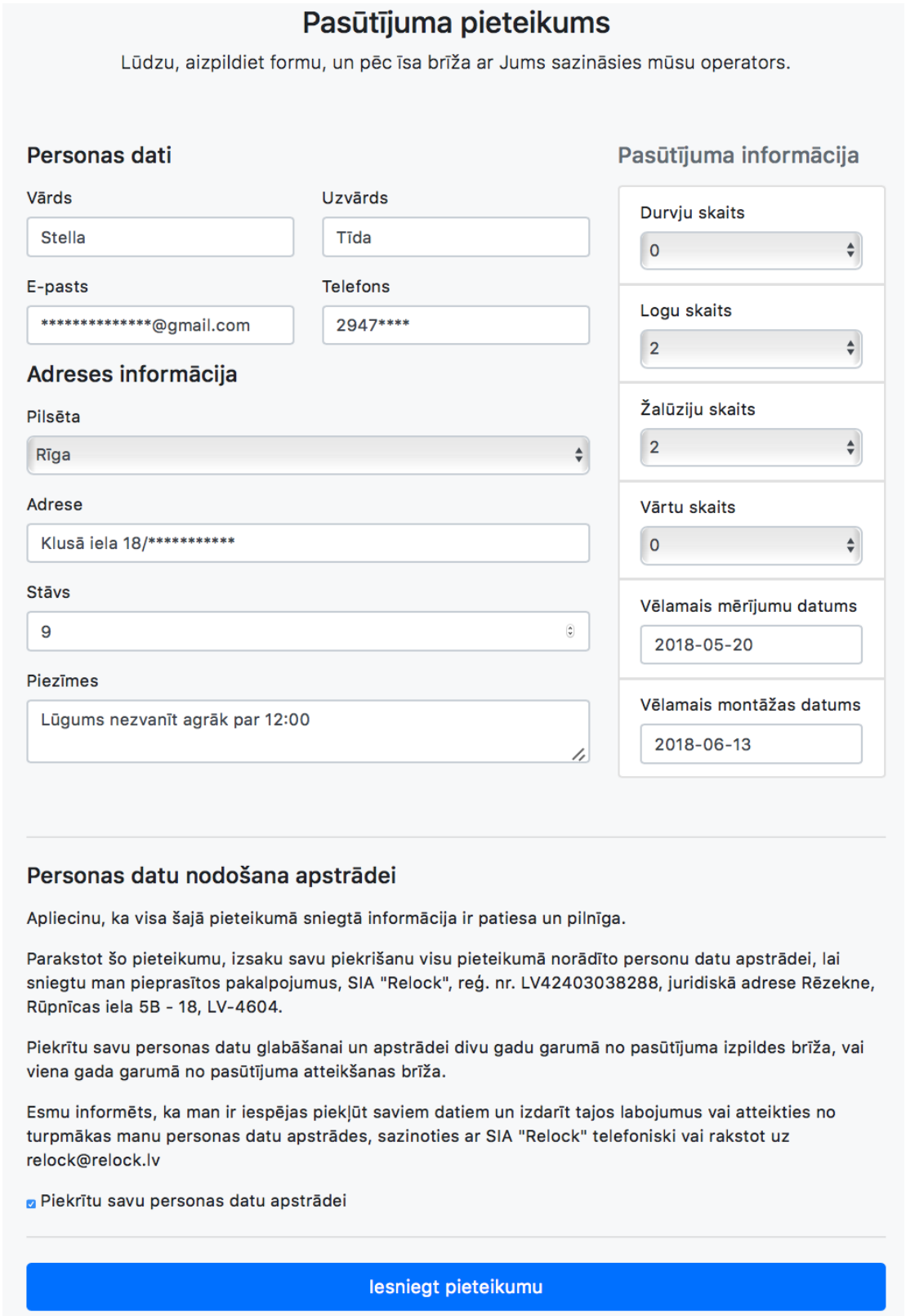
16. *“Tīmekļa lietojumprogrammu drošība*”, bakalaura darbs, Stella Tīda, 2016.

17. *“Personas dati un Vispārīgā datu aizsardzības regula”*, E. Brikmane, Latvijas Vēstneša portāls, 2018. Pieejams: http://m.lvportals.lv/visi/viedokli?id=292782

18. *“Symfony2 Application Security Guidelines”*, University of Pennsylvania. Pieejams: https://www.sas.upenn.edu/computing/infosec_symfony2

PIELIKUMI

1. pielikums. Pasūtījuma pieteikuma forma



Pasūtījuma pieteikums

Lūdzu, aizpildiet formu, un pēc īsa brīža ar Jums sazināsies mūsu operators.

Personas dati

Vārds: Stella

Uzvārds: Tīda

E-pasts: **********@gmail.com

Telefons: 2947****

Adreses informācija

Pilsēta: Rīga

Adrese: Klusā iela 18/**********

Stāvs: 9

Piezīmes: Lūgums nezvanīt agrāk par 12:00

Pasūtījuma informācija

Durvju skaits: 0

Logu skaits: 2

Žalūziju skaits: 2

Vārtu skaits: 0

Vēlamais mērījumu datums: 2018-05-20

Vēlamais montāžas datums: 2018-06-13

Personas datu nodošana apstrādei

Apliecinu, ka visa šajā pieteikumā sniegtā informācija ir patiesa un pilnīga.

Parakstot šo pieteikumu, izsaku savu piekrišanu visu pieteikumā norādīto personu datu apstrādei, lai sniegtu man pieprasītos pakalpojumus, SIA "Relock", reģ. nr. LV42403038288, juridiskā adrese Rēzekne, Rūpnīcas iela 5B - 18, LV-4604.

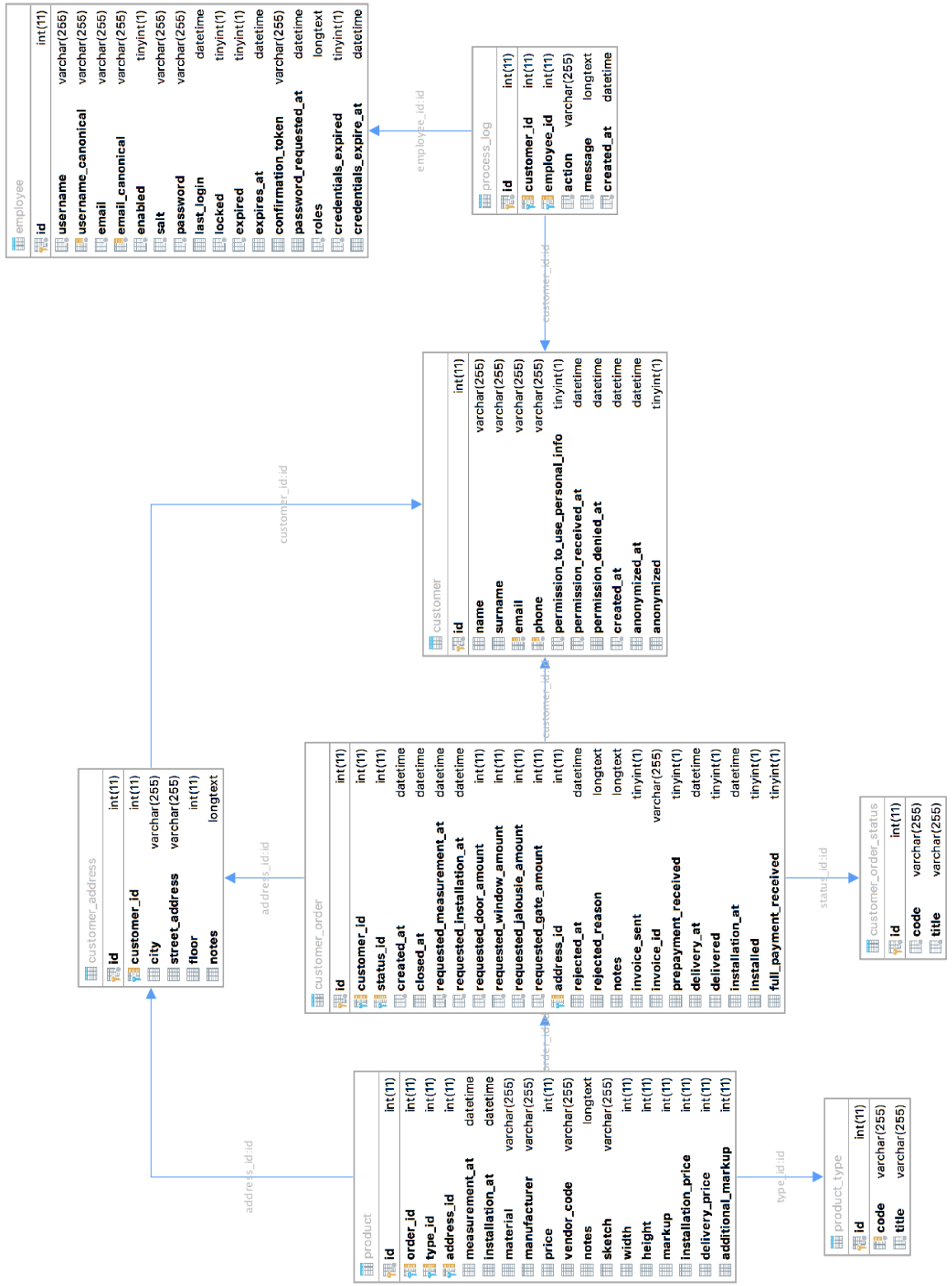
Piekrītu savu personas datu glabāšanai un apstrādei divu gadu garumā no pasūtījuma izpildes brīža, vai viena gada garumā no pasūtījuma atteikšanas brīža.

Esmu informēts, ka man ir iespējas piekļūt saviem datiem un izdarīt tajos labojumus vai atteikties no turpmākas manu personas datu apstrādes, sazinoties ar SIA "Relock" telefoniski vai rakstot uz relock@relock.lv

Piekrītu savu personas datu apstrādei

Iesniegt pieteikumu

2. pielikums. Sistēmas datubāzes shēma



Dokumentārā lapa

Maģistra darbs " UZŅĒMUMA INFORMĀCIJAS SISTĒMAS PIESKAŅOŠANA JAUNAJAI VISPĀRĪGAI DATU AIZSARDZĪBAS REGULAI" izstrādāts LU Datorikas fakultātē.

Darba teksta galīgā versija izgatavota 18.05.2018**.**

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

Autors: _____

(Autora paraksts un datums)

Ar savu parakstu apliecinu, ka esmu lasījis augstāk minēto maģistra darbu un atzīstu to par **p i e m ē r o t u / n e p i e m ē r o t u** (nevajadzīgo svītrot) aizstāvēšanai Latvijas Universitātes datorzinātņu maģistrantūrā.

Darba vadītājs: _____

(Vadītāja paraksts un datums)

Darbs iesniegts **maģistratūras sekretariātā** _____

(Iesniegšanas datums)

Ar šo es apliecinu, ka darba elektroniskā versija ir augšupielādēta LU informatīvajā sistēmā.

Studiju metodiķe: _____

(Metodiķes paraksts)

Recenzents: _____

(Akad.amats, zin.grāds, vārds, uzvārds)

Darbs aizstāvēts maģistra gala pārbaudījuma komisijas sēdē

_____ prot. Nr. _____

(Darba aizstāvēšanas datums)

Komisijas sekretārs: _____

(Sekretāra paraksts)