

KRASSKY PRIVĀTUMA POLITIKA

Šīs Privātuma politikas mērķis ir sniegt fiziskajai personai – SIA “Krassky” (turpmāk – Uzņēmums) klientam – informāciju par personas datu apstrādes nolūku, apjomu, aizsardzību, apstrādes termiņu un datu subjekta tiesībām datu iegūšanas laikā, kā arī apstrādājot klienta personas datus.

PĀRZINIS UN TĀ KONTAKTINFORMĀCIJA

Datu pārzinis, kas ir atbildīgs par Jūsu datu apstrādi, ir SIA “Krassky”, reģ. nr. 40003774722. Uzņēmums ir atbildīgs par Jūsu datu drošu uzglabāšanu, apstrādi un dzēšanu. Ja Jums rodas jautājumi par personas datu apstrādi, lūdzam sazināties ar Uzņēmumu, sūtot e-pastu uz krassky@krassky.lv vai zvanot pa tālruni 67781400.

DOKUMENTA PIEMĒROŠANAS JOMA

Personas dati ir jebkāda informācija par identificētu vai identificējamu fizisku personu. Personas datu kategorijas un piemēri norādīti zemāk:

Datu kategorija	Piemēri
Klienta un sadarbības partnera dati	Vārds, uzvārds, darba vieta un amats, personas kods, bankas konta numurs, adrese, tālruņa numurs, mobilā tālruņa numurs, e-pasts, Facebook adrese, vārda dienas datums, dzimšanas dienas datums, vēlāmā sarunas valoda.
Darba kandidāta (fiziska persona, kas kandidē uz Uzņēmuma darba vakanci) dati	Vārds, uzvārds, tālruņa numurs, e-pasts, LinkedIn profila adrese, saņemtais CV.

Privātuma politiku piemēro privātuma un personas datu aizsardzības nodrošināšanai attiecībā uz zemāk uzskaitītajiem datu subjektiem (turpmāk – Klienti):

- fiziskajām personām – klientiem un citiem Uzņēmuma pakalpojumu lietotājiem (tajā skaitā, potenciālajiem, bijušajiem un esošajiem), kā arī trešajām personām, kuras saistībā ar pakalpojumu sniegšanu fiziskai personai (klientam, partnerim) saņem vai nodod Uzņēmumam jebkādu informāciju (tajā skaitā, kontaktpersonas, maksātāji u.c.);
- Uzņēmuma salonu, biroju, noliktavas un citu telpu apmeklētājiem, tajā skaitā, attiecībā uz kuriem tiek veikta videonovērošana;
- Uzņēmuma uzturēto interneta mājaslapu apmeklētājiem, un zvana veicējiem uz Uzņēmuma vārda reģistrētajiem tālruņiem;
- fiziskajām personām – kandidātiem uz Uzņēmuma brīvajām darba vakancēm.

Uzņēmums rūpējas par Klientu privātumu un personas datu aizsardzību, ievēro Klientu tiesības uz personas datu apstrādes likumību saskaņā ar piemērojamajiem tiesību aktiem - Eiropas Parlamenta un padomes 2016. gada 27. aprīļa [Regulu 2016/679](#) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (turpmāk – Regula) un citiem piemērojamajiem tiesību aktiem privātuma un datu apstrādes jomā.

Privātuma politika ir attiecināma uz datu apstrādi neatkarīgi no tā, kādā formā un/vai vidē Klients sniedz personas datus (interneta mājaslapā, mobilajās lietotnēs, pašapkalpošanās portālā, papīra formātā vai telefoniski) un kādās Uzņēmuma sistēmās vai papīra formā tie tiek apstrādāti.

Attiecībā uz specifiskiem datu apstrādes veidiem (piemēram, sīkdatņu apstrādi u.c.), vidi, nolūkiem var tikt noteikti papildu, specifiski noteikumi, par ko Klients tiek informēts brīdī, kad viņš sniedz attiecīgus datus Uzņēmumam.

PERSONAS DATU APSTRĀDES NOLŪKI

Krassky apstrādā datus šādiem nolūkiem:

- Pakalpojumu sniegšanai un preču pārdošanai:
 - klienta identificēšanai;
 - līguma sagatavošanai, noslēgšanai un noslēgšanas fakta pierādīšanai;
 - preču piegādei un pakalpojumu sniegšanai (līguma saistību izpildei);
 - pakalpojumu darbības nodrošināšanai;
 - garantijas saistību izpildei;



- preču un pakalpojumu uzlabošanai, jaunu preču un pakalpojumu attīstībai;
- pakalpojuma lietošanas veicināšanai, reklamēšanai un izplatīšanai;
- klientu apkalpošanai;
- iesniegumu un iebildumu izskatīšanai un apstrādei;
- klientu noturēšanai, lojalitātes celšanai, apmierinātības mērījumiem;
- norēķinu administrēšanai;
- parādu atgūšanai un piedziņai;
- mājaslapu un mobilo lietotņu uzturēšanai un darbības uzlabošanai.
- Biznesa plānošanai un analītikai:
 - statistikai un biznesa analīzei;
 - plānošanai un uzskaiti;
 - efektivitātes mērīšanai;
 - datu kvalitātes nodrošināšanai;
 - tirgus un sabiedriskā viedokļa pētījumu veikšanai;
 - atskaišu sagatavošanai;
 - klientu aptauju veikšanai;
 - riska vadības aktivitāšu ietvaros.
- Informācijas, informācijas sistēmu un uzņēmuma drošības nodrošināšanai.
- Informācijas sniegšanai valsts pārvaldes iestādēm un operatīvās darbības subjektiem valsts un pašvaldību normatīvajos aktos noteiktajos gadījumos un apjomā.
- Darba vakanču kandidātu atbilstības izvērtēšanai.
- Citos specifiskos nolūkos, par kuriem Klients tiek informēts brīdī, kad viņš sniedz attiecīgus datus Uzņēmumam.

PERSONAS DATU APSTRĀDES TIESISKAIS PAMATS

Uzņēmums apstrādā fiziskas personas datus, balstoties uz šādiem tiesiskajiem pamatiem:

- Klienta piekrišana – Klients, kā personas datu subjekts, pats dod piekrišanu personas datu vākšanai un apstrādei noteiktiem mērķiem. Klienta piekrišana ir viņa brīva griba un patstāvīgs lēmums, kas var tikt sniegts jebkurā brīdī, tādējādi atļaujot Uzņēmumam apstrādāt personas datus noteiktajiem nolūkiem. Klienta piekrišana ir tam saistoša, ja tā tiek sniegta mutiski (telefonsarunas laikā pēc Klienta identifikācijas) vai rakstiski (aizpildot veidlapu Uzņēmuma salonā, nosūtot elektronisko pieprasījumu pēc Klienta identifikācijas). Klientam ir tiesības jebkurā laikā atsaukt savu iepriekš sniegto piekrišanu, izmantojot norādītos saziņas kanālus ar Uzņēmumu. Piekrišanas atsaukums neietekmē apstrādes likumību, kas pamatojas uz piekrišanu pirms atsaukuma.
- Darba kandidāta piekrišana – kandidāts uz vakantu amatu Uzņēmumā, kā personas datu subjekts, pats dod piekrišanu personas datu vākšanai un apstrādei, lai Uzņēmums varētu iespējami precīzi izvērtēt kandidāta atbilstību vakantajam amatam. Darba kandidāta piekrišana ir viņa brīva griba un patstāvīgs lēmums, kas var tikt sniegts jebkurā brīdī, tādējādi atļaujot Uzņēmumam apstrādāt personas datus noteiktajiem nolūkiem. Darba kandidāta piekrišana ir tam saistoša, ja tā tiek sniegta mutiski (telefonsarunas laikā pēc kandidāta identifikācijas) vai rakstiski (aizpildot veidlapu Uzņēmuma salonā, nosūtot elektronisko pieprasījumu). Darba kandidātam ir tiesības jebkurā laikā atsaukt savu iepriekš sniegto piekrišanu, izmantojot norādītos saziņas kanālus ar Uzņēmumu. Piekrišanas atsaukums neietekmē apstrādes likumību, kas pamatojas uz piekrišanu pirms atsaukuma.
- Līguma noslēgšana un izpilde – lai Uzņēmums varētu noslēgt un izpildīt līgumu ar Klientu, kvalitatīvi sniedzot pakalpojumus un apkalpojot Klientu, tam jāapkopo un jāapstrādā noteikti personas dati, kas tiek savākti pirms līguma noslēgšanas ar Uzņēmumu vai jau noslēgtā līguma laikā.
- Juridisko pienākumu izpilde – Uzņēmums ir tiesīgs apstrādāt personas datus, lai izpildītu normatīvo aktu prasības, kā arī sniegtu atbildes uz valsts un pašvaldības likumīgiem pieprasījumiem.
- Vitālu interešu aizsardzība – Uzņēmums ir tiesīgs apstrādāt personas datus, lai aizsargātu Klienta vai citas fiziskas personas vitālas intereses, piem., ja apstrāde ir vajadzīga humanitāros nolūkos, dabas stihiju un cilvēka izraisītu, it īpaši, epidēmiju un to izplatīšanās monitoringam vai ārkārtas humanitārajās situācijās (terora akti, tehnogēnās katastrofu situācijās un tml.).
- Oficiālo pilnvaru izpilde vai sabiedrības intereses – Uzņēmums ir tiesīgs apstrādāt datus, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot Uzņēmumam likumīgi piešķirtās oficiālās pilnvaras. Šādos gadījumos pamats personas datu apstrādei ir iekļauts normatīvajos aktos.
- Uzņēmuma vai trešās personas legītimās (likumīgās) intereses – ievērojot Uzņēmuma intereses, kuru pamatā ir kvalitatīvu pakalpojumu un savlaicīga atbalsta sniegšana Klientam, Uzņēmumam ir tiesības apstrādāt fiziskas personas datus tādā apjomā, kāds tam ir objektīvi nepieciešams un pietiekams šajā Politikā norādītajiem nolūkiem. Uzņēmumam ir šādas legītimās intereses:
 - veikt komercdarbību;
 - sniegt Uzņēmuma pakalpojumus;
 - pārbaudīt Klienta identitāti pirms līguma noslēgšanas;
 - nodrošināt līguma saistību izpildi;

- novērst nepamatotus finansiālus riskus savai komercdarbībai (t.sk., veikt kredītriska novērtējumu pirms preču un pakalpojumu pārdošanas un līguma izpildes laikā);
- saglabāt Klientu pieteikumus un iesniegumus par preču pirkumu un pakalpojumu sniegšanu, citus pieteikumus un iesniegumus, piezīmes par tiem, t.sk., kas veikti rakstveidā vai mutiski, zvanot uz Uzņēmuma telefona numuriem un interneta mājas lapās;
- veikt sarunas ar Klientu ierakstu par pakalpojumu darbības nodrošināšanu, uzturēšanu, norēķiniem, lai veiktu klientu apkalpošanas kvalitātes kontroli;
- veikt sarunas ar Klientu ierakstu, lai organizētu pakalpojuma līgumsaistību izpildi;
- veikt sarunas ar Klientu ierakstu, kuras laikā tiek noslēgts mutisks līgums, līguma noslēgšanas fakta pierādīšanai;
- analizēt Uzņēmuma mājaslapu, interneta vietņu un mobilo lietojumu darbību, izstrādāt un ieviest to uzlabojumus;
- veikt darbības Klientu noturēšanai;
- segmentēt klientu datu bāzi pakalpojumu efektīvākai nodrošināšanai;
- izstrādāt un attīstīt preces un pakalpojumus;
- reklamēt Uzņēmuma preces un pakalpojumus;
- nosūtīt citus ziņojumus par līguma izpildes gaitu un līguma izpildei būtiskiem notikumiem, kā arī veikt Klientu aptaujas par precēm un pakalpojumiem un to lietošanas pieredzi;
- novērst krāpniecību;
- nodrošināt korporatīvo pārvaldību, finanšu un biznesa uzskaiti un analītiku;
- nodrošināt efektīvus uzņēmuma pārvaldības procesus;
- pakalpojumu sniegšanas un preču pārdošanas, un piegādes efektivitāti;
- nodrošināt un uzlabot pakalpojumu kvalitāti;
- administrēt maksājumus;
- administrēt neveiktus maksājumus;
- atlasīt labāko kandidātu darbam Uzņēmumā;
- vērsties valsts pārvaldes un operatīvās darbības iestādēs un tiesā savu tiesisko interešu aizsardzībai;
- informēt sabiedrību par Uzņēmumadarbību.

PERSONAS DATU APSTRĀDE

Uzņēmums apstrādā Klienta datus, izmantojot mūsdienu tehnoloģiju iespējas, ņemot vērā pastāvošos privātuma riskus un Uzņēmumam saprātīgi pieejamos organizatoriskos, finansiālos un tehniskos resursus.

Ar Klientu noslēgtā līguma saistību izpildes kvalitatīvai un operatīvai nodrošināšanai Uzņēmums var pilnvarot savus sadarbības partnerus veikt atsevišķas preču piegādes vai pakalpojumu sniegšanas darbības, kā piemēram, preču piegādes veikšanu, rēķinu izsūtīšanu un tamlīdzīgi. Ja izpildot šos uzdevumus, sadarbības partneri apstrādā Krassky rīcībā esošos Klienta personas datus, attiecīgie sadarbības partneri ir uzskatāmi par Krassky datu apstrādes operatoriem (apstrādātājiem) un Uzņēmumam ir tiesības nodot sadarbības partneriem šo darbību veikšanai vajadzīgos Klienta personas datus tādā apmērā, kā tas nepieciešams šo darbību veikšanai.

Uzņēmuma sadarbības partneri (personas datu apstrādātāja statusā) nodrošinās personas datu apstrādes un aizsardzības prasību izpildi saskaņā ar Uzņēmuma prasībām un tiesību aktiem, un neizmantos personas datus citos nolūkos, kā tikai ar Klientu noslēgtā līguma/vienošanās saistību izpildei Krassky uzdevumā.

PERSONAS DATU AIZSARDZĪBA

Uzņēmums aizsargā Klienta datus, izmantojot mūsdienu tehnoloģiju iespējas, ņemot vērā pastāvošos privātuma riskus un Uzņēmuma saprātīgi pieejamos organizatoriskos, finansiālos un tehniskos resursus, tajā skaitā izmantojot šādus drošības pasākumus:

- Datu šifrēšanu, pārraidot datus (SSL šifrēšana);
- Datu šifrēšanu serveros;
- Ugunsmūri;
- Ielaušanās aizsardzības un atklāšanas programmas;
- Citus aizsardzības pasākumus atbilstoši aktuālajām tehnikas attīstības iespējām.

PERSONAS DATU SAŅĒMĒJU KATEGORIJAS

Uzņēmums neizpauž trešajām personām Klienta personas datus vai jebkādu pakalpojumu sniegšanas un līguma darbības laikā iegūtu informāciju, tajā skaitā, informāciju par saņemtajiem pakalpojumiem, izņemot:

- ja attiecīgajai trešajai personai dati jānodod noslēgtā līguma ietvaros, lai veiktu kādu līguma izpildei nepieciešamu vai ar likumu deleģētu funkciju (piemēram, bankai norēķinu ietvaros vai nodrošinātu pakalpojumu, piemēram, preču piegādi, par ko Klients tiek informēts);
- saskaņā ar Klienta skaidru un nepārprotamu piekrišanu;
- ārējos normatīvajos aktos paredzētajām personām pēc viņu pamatota pieprasījuma, ārējos normatīvajos



- aktos noteiktajā kārtībā un apjomā;
- ārējos normatīvajos aktos noteiktos gadījumos Krassky leģitīmo interešu aizsardzībai, piemēram, vērsoties tiesā vai citās valsts institūcijās pret personu, kura ir aizskārusi šīs Uzņēmuma leģitīmās intereses.

PERSONAS DATU GLABĀŠANAS ILGUMS

Uzņēmums glabā un apstrādā Klienta personas datus, kamēr pastāv vismaz viens no šiem kritērijiem:

- tikai tik ilgi, kamēr ir spēkā ar Klientu noslēgtais līgums (tajā skaitā, sarunu, kurās tiek noslēgts mutisks līgums / izdarīts pakalpojuma pieteikums, ierakstus);
- dati ir nepieciešami tam nolūkam, kam tie ir saņemti;
- kamēr ārējos normatīvajos aktos noteiktajā kārtībā Krassky vai Klients var realizēt savas leģitīmās intereses (piemēram, iesniegt iebildumus vai celt vai vest prasību tiesā);
- kamēr kādai no pusēm pastāv juridisks pienākums datus glabāt (piemēram, saskaņā ar Latvijas Republikas normatīvajiem aktiem, uzņēmumam rēķini jāglabā 5 gadus, u.c.);
- kamēr ir spēkā Klienta piekrišana attiecīgai personas datu apstrādei, ja nepastāv cits datu apstrādes likumīgs pamats.
- Pēc tam, kad šajā punktā minētie apstākļi izbeidzas, Klienta personas dati tiek dzēsti. Auditācijas pieraksti tiek uzglabāti vismaz vienu gadu no to veikšanas dienas saskaņā ar normatīvajos aktos noteikto.

PIEKĻUVE PERSONAS DATIEM UN CITAS KLIENTA TIESĪBAS

Klientam saskaņā ar normatīvajiem aktiem ir tiesības pieprasīt Krassky piekļuvi saviem personas datiem, kā arī pieprasīt Uzņēmumam veikt to papildināšanu, labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz Klientu, vai tiesības iebilst pret apstrādi (tajā skaitā pret personas datu apstrādi, kas veikta pamatojoties uz Uzņēmuma leģitīmajām interesēm), kā arī tiesības uz datu pārnesamību. Šīs tiesības īstenojamās, ciktāl datu apstrāde neizriet no Krassky pienākumiem, kas tam ir uzlikti ar spēkā esošajiem normatīvajiem aktiem, un kuri tiek veikti sabiedrības interesēs.

Klients var iesniegt pieprasījumu par savu tiesību īstenošanu:

- rakstveida formā klātienē Uzņēmuma salonā Duntes ielā 3, Rīgā, uzrādot personu apliecinošu dokumentu;
- elektroniskā pasta veidā, sūtot pieprasījumu uz krassky@krassky.lv un parakstot to ar drošu elektronisko parakstu.

Saņemot Klienta pieprasījumu par savu tiesību īstenošanu, Krassky pārliecinās par Klienta identitāti, izvērtē pieprasījumu un izpilda to saskaņā ar normatīvajiem aktiem.

Uzņēmums atbildi Klientam nosūta pa pastu uz viņa norādīto kontaktadresi ierakstītā vēstulē vai ņemot vērā Klienta norādīto atbildes saņemšanas veidu.

Krassky nodrošina datu apstrādes un aizsardzības prasību izpildi saskaņā ar normatīvajiem aktiem un Klienta iebildumu gadījumā veic lietderīgās darbības, lai iebildumu atrisinātu. Tomēr, ja tas neizdodas, Klientam ir tiesības vērsties uzraudzības iestādē - Datu valsts inspekcijā.

KLIENTA PIEKRIŠANA DATU APSTRĀDEI UN TIESĪBAS TO ATSAUKT

Klients piekrišanu personas datu apstrādei, kuras tiesiskais pamats ir piekrišana, var dot Uzņēmuma interneta lapās (piemēram, jaunumu saņemšanas pierakstīšanas formas), zvanot vai klātienē Uzņēmuma salonos.

Klientam ir tiesības jebkurā brīdī atsaukt datu apstrādei doto piekrišanu tādā pat veidā, kādā tā dota, tas ir – zvanot, nosūtot elektronisko pastu vai klātienē Krassky salonos, un tādā gadījumā turpmāka datu apstrāde, kas balstīta uz iepriekš doto piekrišanu konkrētajam nolūkam netiks veikta.

Piekrišanas atsaukums neietekmē datu apstrādes, kuras veiktas tajā laikā, kad Klienta piekrišana bija spēkā.

Atsaucot piekrišanu, nevar tikt pārtraukta datu apstrāde, kuru veic, pamatojoties uz citiem tiesiskajiem pamatiem.

SAZIŅA AR KLIENTU

Uzņēmums veic saziņu ar Klientu, izmantojot Klienta norādīto kontaktinformāciju (telefona numuru, e-pasta adresi, pasta adresi).

Saziņu par pakalpojumu līgumsaistību izpildi Uzņēmums veic uz noslēgtā līguma pamata (piemēram, preču vai pakalpojumu piegādes, informācija par rēķiniem, izmaiņām pakalpojumos u.c.).

KOMERCIĀLI PAZIŅOJUMI

Saziņu par komerciāliem paziņojumiem par Uzņēmuma un/vai trešo pušu pakalpojumiem un citiem ar tiešu nolīgto pakalpojumu nodrošināšanu nesaistītiem paziņojumiem (piemēram, klientu aptaujas) Krassky veic saskaņā ar ārējos normatīvajos aktos noteikto vai saskaņā ar Klienta piekrišanu.

Klients piekrišanu Uzņēmumam un/vai tā sadarbības partneru komerciālu paziņojumu saņemšanai var dot



Uzņēmuma interneta lapās (piemēram, jaunumu saņemšanas pierakstīšanas formas), zvanot vai klātienē Uzņēmuma salonos.

Klienta dotā piekrišana komerciālu paziņojumu saņemšanai ir spēkā līdz tās atsaukumam (arī pēc pakalpojumu līguma izbeigšanās). Klients jebkurā laikā var atteikties no turpmākas komerciālo paziņojumu saņemšanas kādā no šādiem veidiem:

- nosūtot e-pastu uz adresi krassky@krassky.lv;
- zvanot pa tālruni 67781400;
- klātienē Uzņēmuma salonos;
- izmantojot komerciālajā paziņojumā paredzēto automatizēto iespēju atteikties no turpmāku paziņojumu saņemšanas, noklikšķinot uz atteikšanās norādes attiecīgā komerciālā paziņojuma (e-pasta) beigās.

Uzņēmums pārtrauc komerciālo paziņojumu sūtīšanu, tiklīdz tiek apstrādāts Klienta pieprasījums. Pieprasījuma apstrāde ir atkarīga no tehnoloģiskām iespējām, kas var būt līdz septiņām diennaktīm.

Izsakot savu viedokli aptaujās un atstājot savu kontaktinformāciju (e-pastu, tālruni), Klients piekrīt, ka Krassky var ar viņu sazināties sakarā ar Klienta sniegto novērtējumu, izmantojot Klienta atstāto kontaktinformāciju.

SĪKDATŅU IZMANTOŠANA KRASSKY INTERNETA VIETNĒS

Uzņēmuma mājaslapas izmanto sīkdatnes. Sīkdatnes ir mazas teksta datnes, kuras tīmekļa pārlūkprogramma (piemēram, Chrome, Mozilla Firefox, Safari u.c.) saglabā lietotāja galiekārtā (datorā, mobilajā tālrunī, planšetē) brīdī, kad lietotājs apmeklē tīmekļa vietni, lai identificētu pārlūkprogrammu vai pārlūkprogrammā saglabātu informāciju vai iestatījumus. Tādējādi ar sīkdatņu palīdzību tīmekļa vietne iegūst spēju saglabāt lietotāja individuālos iestatījumus, atpazīt viņu un atbilstoši reaģēt, ar mērķi uzlabot vietnes lietošanas pieredzi. Lietotājs var atspējot vai ierobežot sīkdatņu izmantošanu, taču bez sīkdatnēm nebūs iespējams pilnvērtīgi izmantot visas vietņu funkcijas.

Atkarībā no veicamajām funkcijām un izmantošanas mērķa, Uzņēmums izmanto šādas sīkdatnes:

- **Obligātās sīkdatnes**
Šīs sīkdatnes nepieciešamas, lai lietotājs varētu brīvi apmeklēt un pārlūkot tīmekļa vietni un izmantot tās piedāvātās iespējas, tajā skaitā iegūt informāciju par jaunumiem un produktiem. Šīs sīkdatnes identificē lietotāja iekārtu, taču neizpauž lietotāja identitāti, kā arī tās nevāc un neapkopo informāciju. Bez šīm sīkdatnēm tīmekļa vietne nevarēs pilnvērtīgi darboties, piemēram, sniegt lietotājam nepieciešamo informāciju. Šīs sīkdatnes tiek glabātas lietotāja iekārtā līdz brīdim, kad tiek aizvērta tīmekļa pārlūkprogramma.
- **Funkcionālās sīkdatnes**
Ar funkcionālajām sīkdatnēm vietne atceras lietotāja izvēlētos uzstādījumus un veiktās izvēles, lai lietotājs varētu ērtāk lietot vietni. Šīs sīkdatnes glabājas lietotāja iekārtā pastāvīgi.
- **Analītiskās sīkdatnes**
Analītiskās sīkdatnes apkopo informāciju par to, kā lietotājs lieto tīmekļa vietni, konstatē biežāk apmeklētās sadaļas, ieskaitot saturu, kuru lietotājs izvēlas, pārlūkojot vietni. Informācija tiek lietota analīzes nolūkos, lai noskaidrotu, kas interesē vietnes lietotājus, un varētu uzlabot vietnes funkcionalitāti, padarot to ērtāk lietojamu. Analītiskās sīkdatnes identificē tikai lietotāja iekārtu, taču neizpauž lietotāja identitāti. Atsevišķos gadījumos dažas no analītiskajām sīkdatnēm vietnes īpašnieka vietā, saskaņā ar tā norādījumiem un tikai atbilstoši norādītajiem mērķiem, pārvalda trešās personas - datu apstrādātāji (operatori), piemēram, Google Analytics.
- **Mērķa (reklāmas) sīkdatnes**
Mērķa (reklāmas) sīkdatnes izmanto, lai apkopotu informāciju par lietotāja apmeklētajām tīmekļa vietnēm un piedāvātu tieši konkrētam lietotājam interesējošus Uzņēmuma vai sadarbības partneru produktus vai adresētu konkrētā lietotāja izrādītajai interesei atbilstošus piedāvājumus. Parasti šīs sīkdatnes ar vietnes īpašnieka atļauju atbilstoši norādītajiem mērķiem izvieto trešās personas, piemēram, Google Ads. Mērķa sīkdatnes lietotāja galiekārtā tiek uzglabātas pastāvīgi.

Krassky izmanto sīkdatnes šādiem mērķiem:

- uzlabotu vietņu un mājaslapu lietošanas pieredzi;
- nodrošinātu mājaslapas funkcionalitāti;
- pielāgotu mājaslapas funkcionalitāti lietotāja lietošanas paradumiem - tai skaitā valodai, meklēšanas pieprasījumiem, iepriekš apskatītajam saturam;
- iegūtu statistikas datus par lapas apmeklētāju plūsmu - apmeklētāju skaitu, lapā pavadīto laiku, ģeogrāfisko piederību, lietoto ierīci u.c.;



- piedāvātu Uzņēmuma radītu vai izplatītu saturu un piedāvājumus.

Sīkdatņu glabāšanas laiks

Ja nav noteikts citādi, sīkdatnes tiek glabātas, kamēr tiek izpildīta darbība, kādam nolūkam tās vāktas, un pēc tam tās tiek dzēstas.

Sīkdatņu informācija netiek nodota apstrādei ārpus Eiropas Savienības un EEZ valstīm.

Sīkdatņu apstiprināšana un atspējošana

Apmeklējot Uzņēmuma vietnes un mājaslapas, lietotājam tiek attēlots logs ar ziņojumu par to, ka tīmekļa vietnē tiek izmantotas sīkdatnes. Aizverot šo ziņojuma logu, lietotājs apstiprina, ka ir iepazinies ar informāciju par sīkdatnēm, to izmantošanas nolūkiem, gadījumiem, kad to informācija tiek nodota trešajai personai, un tiem piekriņ. Attiecīgi, sīkdatņu izmantošanas tiesiskais pamats ir lietotāja piekrišana. Ikvienas tīmekļa pārlūkprogrammas drošības iestatījumos iespējama sīkdatņu ierobežošana un dzēšana. Tomēr jāņem vērā, ka nevar atteikties no obligāto un funkcionālo sīkdatņu lietošanas, jo bez tām vietnes un mājaslapas pilnvērtīgas lietošanas nodrošināšana nav iespējama.

Krassky mājaslapās var tikt ievietotas saites uz trešo personu interneta mājaslapām, kurām ir savi lietošanas un personas datu aizsardzības noteikumi, par ko Uzņēmums nenes atbildību.

CITI NOTEIKUMI

Uzņēmumam ir tiesības veikt papildinājumus Privātuma politikā, padarot pieejamu Klientam tās aktuālo versiju Uzņēmuma mājaslapā – www.krassky.lv.



KRASSKY VIDEONOVĒROŠANAS SISTĒMAS

DROŠĪBAS NOTEIKUMI

1. Lietotie termini:

Pārzinis - SIA "Krassky", vienotais reģistrācijas Nr.540003774722, juridiskā adrese Duntē ielā 3, Rīgā, turpmāk – Sabiedrība.

Objekts – Krassky salons 1. stāvā un 6 stāvā Rīgā, Duntē ielā 3, biroja telpas 2.stāvā un 4.stāvā, Rīgā, Duntē ielā 3.

Vispārīgā datu aizsardzības regula - 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).

Videonovērošanas sistēma - Videoierakstu veikšana ar videonovērošanas kamerām un aplūkošana tiešsaistes sistēmā, kā rezultātā iegūst identificējamu personu attēlus vai citu informāciju, kas attiecas uz identificējamām fiziskām personām.

Atbildīgā persona – SIA "Krassky" darbinieks pēc rīkojuma.

2. Vispārīgie noteikumi

2.1. Sabiedrības Videonovērošanas sistēmas drošības noteikumi (turpmāk – Noteikumi) nosaka kārtību, kādā Objektā veic personas datu – attēla un skaņas apstrādi Videonovērošanas sistēmā, tās vispārīgās tehniskās un organizatoriskās prasības atbilstoši normatīvo aktu prasībām, kas regulē fizisko personu datu aizsardzību.

2.2. Noteikumi nosaka:

- 2.2.1. ar kādiem tehniskajiem resursiem nodrošina personas datu apstrādi un drošību;
- 2.2.2. kāds ir videonovērošanas ierakstu glabāšanas ilgums;
- 2.2.3. kuros gadījumos un kādā kārtībā ir atļauta piekļuve videonovērošanai tiešsaistes režīmā un videonovērošanas kameru ierakstu arhīvam;
- 2.2.4. kāda ir videonovērošanas drošības prasību ievērošana ikdienā;
- 2.2.5. par tehniskajiem jautājumiem atbildīgo personu;
- 2.2.6. brīdinājuma zīmju par videonovērošanas veikšanu izvietošanu.

2.3. Sabiedrība, veicot videonovērošanu:

- 2.3.1. vadās no vienotas izpratnes un aizsardzības prasībām attiecībā uz videonovērošanu kā fizisko personu datu apstrādes veidu;
- 2.3.2. izvairās no riskiem un iespējamiem pārkāpumiem, kas saistīti ar fizisko personu datu apstrādi, kas Sabiedrībai var radīt tiesiski un/vai materiāli nelabvēlīgas sekas.

2.4. Noteikumi izstrādāti pamatojoties uz Vispārīgo datu aizsardzības regulu un citiem fiziskas personas datu aizsardzību regulējošiem normatīvajiem aktiem, kā arī Datu valsts inspekcijas rekomendācijām un vadlīnijām datu apstrādei videonovērošanas jomā un personas datu aizsardzībai darba vietā.

2.5. Noteikumi ir saistoši visiem Videonovērošanas sistēmas lietotājiem - Sabiedrības valdei, Atbildīgajai personai, darbiniekiem, kuri veic videonovērošanas attēla tiešskati un uzraudzību vai citām personām, kurām Sabiedrība noteiktos gadījumos piešķirusi attiecīgu piekļuvi darbam ar Videonovērošanas sistēmu, kā arī tie apņemas ievērot iekārtu programmas lietošanas instrukcijās norādītās prasības.

2.6. Videonovērošanas sistēmas iekārtas un videokameras ir uzstādītas tādas, lai nodrošinātu attēla nolūkam un audio atbilstošu kvalitāti, ņemot vērā tehnisko specifikāciju un vietu vai vidi, kur tās ir novietotas.

2.7. Ja videonovērošanas laikā neiegūst attēlu, no kura ir iespējams identificēt datu subjektu (attēlam ir zema izšķirtspēja), tad šo Noteikumu prasības, kas attiecas uz fizisko personu datu aizsardzību, nav piemērojamas.

2.8. Videonovērošanas kameras nedrīkst izmantot, lai ierakstītu sarunas starp cilvēkiem. Iekārtas ir bez audioieraksta esamības, vai arī tā ir jāatslēdz. Atbildīgā persona nodrošina, ka, veicot videonovērošanu, netiek veikts audioieraksts.

3. Videonovērošanas mērķis

3.1. Videonovērošanas mērķis ir noziedzīgu nodarījumu novēršana un atklāšana, personu dzīvības, veselības un īpašuma aizsardzība, kā arī citu sabiedrības individu interešu ievērošana un sabiedriskās kārtības nodrošināšana.



- 3.2. Sabiedrība, ņemot vērā to, ka Objekts ir sabiedriskā vieta, ko apmeklē plašs personu loks, kā arī Objektā tiek organizēti pasākumi ar paaugstinātas drošības prasībām, ir guvusi pārliecību, ka videonovērošanas veikšanas ieguvums būs lielāks, nekā fiziskajai personai nodarītais privātuma apdraudējums un, ka tā nodrošinās Noteikumu 3.1.punktā norādītā mērķa sasniegšanu tādā veidā, kas vismazāk aizskar personas tiesības uz privātumu.
- 3.3. Veicot videonovērošanu, tiek ievērots ārējos normatīvajos aktos un Noteikumos noteiktais videonovērošanas kā datu apstrādes veida regulējums.

4. Tehniskie resursi, ar kādiem nodrošina personas datu apstrādi un drošību

- 4.1. Personu datus ievāc, izmantojot videonovērošanas kameras, kas darbojas nepārtraukti.
- 4.2. Personu datu apstrādei Objektā izmanto 26 iekšējās izvietotas kameras.
- 4.3. Lietojot tehniskos resursus, Sabiedrība tos izmanto atbilstoši ražotāja noteiktajām prasībām, un to pareiza lietošana nodrošina Videonovērošanas sistēmas drošību un darbību.
- 4.4. Sistēmas darbību nodrošina video ieraksta ierīce un informācijas uzglabāšanu cietajā diskā līdz 15 (piecpadsmit) dienām.
- 4.5. Ierakstu informācija ir pieejama tikai Atbildīgajai personai un Sabiedrības valdes loceklim.
- 4.6. Piekļuve tehniskajiem resursiem ir tikai Atbildīgajai personai. Atbildīgā persona, normatīvajos aktos noteiktajos gadījumos, var ierakstīto informāciju nodemonstrēt citai personai, aizpildot šo noteikumu 6.5. punktā minēto informāciju, ja pirms tam ir saņemta Sabiedrības valdes locekļa atļauja, kurā norādīts iemesls šādu datu izpaušanai.
- 4.7. Atbildīgā persona, saņemot tiesībsargājošo institūciju rakstveida pieprasījumu par videoieraksta izsniegšanu, sagatavo pieprasītā videoieraksta fragmenta ierakstu aizpilda šo noteikumu 6.5. punktā minēto informāciju.
- 4.8. Sabiedrība izmanto programmatūru, saskaņā ar attiecīgās programmatūras licencē norādītajām prasībām.
- 4.9. Telpā, kurā veic personas datu apstrādi (servera vai datora atrašanās vieta):
 - 4.9.1. temperatūra ir ne mazāka kā +10 C un ne vairāk kā +30 C;
 - 4.9.2. fiziskie apstākļi datu nesēja iekārtai tiek uzturēti, nodrošinot telpā apkuri un ventilāciju;
 - 4.9.3. ir uzstādītas pārvietojamās ugunsdzēsīgamās iekārtas;
 - 4.9.4. tehnisko resursu darbības nepārtrauktību nodrošina nepārtrauktās barošanas iekārta (UPS).
- 4.10. Sistēmas ierakstu rezerves kopiju veikšana nav obligāta. Lēmumu par nepieciešamību nodrošināt rezerves kopijas pieņem atbildīgā persona par informācijas sistēmas drošību.
- 4.11. Atbildīgā persona nodrošina, ka pie visām objekta ieejām ir izvietots informatīvs paziņojums par videonovērošanas veikšanu (1. pielikums).

5. Videonovērošanas ierakstu glabāšanas vieta un ilgums

- 5.1. Pēc vērtības informācija ir uzskatāma par vidēji augstas vērtības informāciju.
- 5.2. Pēc konfidencialitātes informācija ir uzskatāma par ierobežotas pieejamības informāciju.
- 5.3. Videonovērošanas ierakstu dati klasificējami kā ierobežotas pieejamības informācija, kurai drīkst piekļūt tikai Atbildīgā persona.
- 5.4. Videonovērošanas sistēmas ierakstu glabāšanas ilgums ir līdz 15 (piecpadsmit) diennaktīm. Pēc minētā termiņa beigām ieraksti tiek dzēsti automātiski hronoloģiskā secībā no ieraksta brīža.
- 5.5. Videoieraksti no Objektā veiktās videonovērošanas glabājas Objektā uz vietas esošajā videoieraksta iekārtā. Ja veic Videonovērošanas sistēmas apkopes darbus vai remontu, Atbildīgā persona nodrošina videonovērošanas ieraksta arhīva pārvietošanu uz ārējo informācijas nesēju.

6. Drošības pasākumi attiecībā uz piekļuvi videonovērošanas sistēmai

- 6.1. Lai nodrošinātu Sabiedrības uzstādīto Videonovērošanas sistēmas un videoieraksta iekārtas esošo datu drošību un fiksētu visus datu apskates un kopēšanas gadījumus, ievēro šādas prasības:
 - 6.1.1. Videonovērošanas sistēmu veiktie ieraksti tiek veikti elektroniski un tiek glabāti ne ilgāk kā 15 (piecpadsmit) diennaktis no ieraksta brīža. Ieraksti tiek dzēsti automātiski hronoloģiskā secībā no ieraksta brīža, Ja ir konstatēti pretiesiski nodarījumi un videoieraksti ir nepieciešami to atklāšanai, datus uzglabā tik ilgi, cik tas ir nepieciešams;
 - 6.1.2. Sabiedrība ir norīkojusi Atbildīgo personu piekļuvei Videonovērošanas sistēmai un tajā esošajiem personas datiem (ierakstiem);
 - 6.1.3. Jebkāda veida Videonovērošanas sistēmas ieraksta iekārtā esošo personas datu (ierakstu) manuāla dzēšana, kopēšana vai nodošana datu subjektam vai tiesībsargājošām iestādēm notiek tikai pēc kompetenta valsts iestādes rakstveida pieprasījuma. Ieraksta dzēšana, kopēšana vai nodošana trešajām personām ir veicama tikai ar Sabiedrības valdes locekļa rakstisku atļauju, aizpildot šo noteikumu 6.5. punktā minēto informāciju.
- 6.2. Piekļuve videoierakstiem no videonovērošanas kamerām ir ierobežota, un tā iedalās divos veidos:

- 6.2.1. tiešsaistes skatīšanās režīms;
- 6.2.2. arhīva skatīšanās režīms.
- 6.3. Piekļuve visām Sabiedrības uzstādītajām Videonovērošanas sistēmām tiešsaistes skatīšanās režīmā ir administratoriem un Atbildīgajai personai.
- 6.4. Arhīva skatīšanās režīms ir pieejams Atbildīgajai personai un Sabiedrības valdes loceklim. Videonovērošanas sistēmas administratora tiesības ir tikai Atbildīgajai personai.
- 6.5. Attiecīgās registrācijas lapās, ja ir nepieciešams nodot datus, fiksē šādus gadījumus:
 - 6.5.1. videoieraksta iekārtā esošo datu (ierakstu) apskate (2.pielikums);
 - 6.5.2. videoieraksta iekārtā esošo datu (ierakstu) kopēšana uz citiem datu nesējiem (3.pielikums);
 - 6.5.3. videoieraksta iekārtā esošo datu (ierakstu) nodošanu, datu subjektam, trešajām personām un tiesībsargājošām iestādēm (2.pielikums).
 - 6.5.4. videoieraksta dzēšana (4.ielikums).
- 6.6. Sabiedrības rīcībā esošos videonovērošanas kameru ierakstus, atbilstoši ārējiem normatīvajiem aktiem, ir tiesīgi pieprasīt un saņemt noteiktās iestādes savu normatīvajos aktos noteikto pienākumu veikšanai.
- 6.7. Datu subjekts ir tiesīgs pieprasīt videonovērošanas ierakstus, taču tikai tādus, kas attiecas uz šo datu subjektu. Ja videoierakstā ir redzama un identificējama cita fiziska persona, Sabiedrībai ir jānodrošina, ka tās dati (attēls) netiek izpausti, piemēram, padarot šo attēlu nesaskatāmu. Ja videoieraksts ir vairākas stundas ilgs, bet datu subjekts tajā redzams vien dažas minūtes, viņam ir izsniedzama tikai šī ieraksta daļa.

7. Ārkārtas apstākļi

- 7.1. Ārkārtas apstākļu gadījumā Videonovērošanas sistēmas darbības aizsardzība notiek saskaņā ar telpu ugunsdrošības noteikumiem. Iespēju gadījuma tehniskie resursi, kuros glabā personu datus, jānogādā drošā vietā.
- 7.2. Sabiedrība nodrošina pietiekamu dokumentāciju, lai varētu izdarīt izmaiņas sistēmā vai arī pilnībā atjaunot sistēmu apdraudējuma iestāšanās gadījumā.
- 7.3. Ārkārtas apstākļu gadījumā Videonovērošanas sistēmas darbības atjaunošanai izmanto līdzīgus tehniskos resursus.

8. Līdzekļi, ar kādiem nodrošina tehniskos resursus pret tīšu bojāšanu un neatļautu iegūšanu

- 8.1. Telpu apsardzi nodrošina Sabiedrība. Telpās ir tehniskā apsardze ar pieslēgšanu diennakts novērošanas pultij, t.sk. ugunsdrošības signalizācijas sistēmas un trauksmes pogas un fiziskās apsardzes postenis (diennakti).
- 8.2. Sistēmas tehniskie resursi tiek saglabāti, slēdzot telpas pēc darba laika beigām.
- 8.3. Telpās, kurās veic personas datu apstrādi (atrodas serveris vai dators, kurā glabājas ieraksts) nav pieejamas nepiederošām personām.
- 8.4. Parole piekļuvei personas datiem (ierakstiem) ir zināma tikai Atbildīgajai personai.
- 8.5. Personu datu apstrādes loģisko drošību nodrošina uzstādītā satura vadības sistēma, kas neļauj personas datus labot vai dzēst bez sankcionētas pieejas. Pieeja datu rediģēšanai pieejama tikai konkrētajam personas datu subjektam.

9. Datu subjekta tiesības saņemt videonovērošanas datus

- 9.1. Datu subjektam ir tiesības piekļūt informācijai attiecībā uz videonovērošanu, kas ir Pārziņa rīcībā (tai skaitā, ja tā ir tehniski pieejama), bet to nav iespējams labot vai papildināt, jo pretējā gadījumā tā tiks uzskatīta par informācijas viltošanu vai sagrozīšanu.
- 9.2. Atbildīgā persona nodrošina videomateriāla kopijas rezervēšanu, izrakstot videomateriālu no lokālā video arhīva:
 - 9.2.1. saņemot pieprasījumu Sabiedrība to reģistrē un nodod izpildei Atbildīgajai personai. Tiesībsargājošā iestāde apstiprina pieprasītās informācijas saņemšanu, apliecinot to ar konkrētās personas vārdu, uzvārdu, amatu, datumu, uz datu nesēja informācijas. Pieprasījums ar minēto apliecinājumu glabājas Sabiedrības nomenklatūras lietā;
 - 9.2.2. ja ir saņemta personas sūdzība tai skaitā anonīma, ko Atbildīgā persona, kontekstā ar videonovērošanas nolūkiem, ir novērtējis kā pietiekamu datu rezerves pieprasījuma apstrādi (piem., ja subjekts klātienē nav identificēts, bet saņemts anonīmais ziņojums, ka ir novērots ka darbinieks ir veicis prettiesiska labuma pieņemšanu);
 - 9.2.3. ja ir iestājies notikums, kas automātiski informē par drošības incidenta pazīmēm vai, ja Atbildīgā persona ir veikusi rezervācijas pieprasījumu saskaņā ar iekšējās kontroles prasībām;
 - 9.2.4. ja no datu subjekta saņem rakstveida iesniegumu, kas satur informāciju pieprasīto datu identificēšanai, un datu subjekts klātienē ir identificēts saskaņā ar 9.5.punktā noteiktajām prasībām.

- 9.3. Atbildīgā persona datu subjektam izsniedz foto fiksāciju/-as no videomateriāla, neatklājot citu personu foto fiksācijas datus un videomateriāla aprakstu un/vai audioieraksta izklāstu, neatklājot citu personu audioieraksta datus. Datu subjektam izsniedz to foto fiksāciju, kas visvairāk atbilst videonovērošanas datu pieprasījuma pamatojumam.
- 9.4. Ja datu subjekts nav identificēts pirms rezervācijas pieprasījuma saņemšanas, tad datu subjektam videonovērošanas datus izsniedz tikai tādā gadījumā, ja datu subjekts ir iesniedzis rakstisku iesniegumu un datu subjektu identificē klātienē.
- 9.5. Lai datu subjekts saņemtu videonovērošanas datus, tas ierodas pie Atbildīgās personas objektā vai pie Sabiedrības tās juridiskajā adresē:
- 9.5.1. Datu subjekts Atbildīgajai personai vai Sabiedrības darbiniekam uzrāda personu apliecinošu dokumentu, iesniedz rakstveida iesniegumu, norādot:
- 9.5.1.1. videonovērošanas datu pieprasīšanas pamatojumu;
 - 9.5.1.2. datumu, laiku un vietu (tai skaitā videokameras atrašanās vietu, ja tā ir zināma), kur videomateriāls uzņemts;
 - 9.5.1.3. situācijas vai notikuma aprakstu (kurā fiksēti datu subjekta videonovērošanas dati);
 - 9.5.1.4. detalizēts datu subjekta vizuālā izskata aprakstu, kas ietver informāciju par apģērbu un mantām, kas atradās pie datu subjekta, un konkrētu datu subjekta atrašanās vietu, kurā datu subjekts bija atradies;
 - 9.5.1.5. citu informāciju, kas ir būtiska pieprasīto datu identificēšanai;
 - 9.5.1.6. vēlamo videonovērošanas datu saņemšanas termiņu;
 - 9.5.1.7. ja videonovērošanas datus nav iespējams izsniegt uzreiz, iesniedz vienu krāsainu fotogrāfiju, kur datu subjekts redzams pilnā augumā un pēc kuras datu subjektu var vizuāli identificēt atbilstoši personu apliecinošajā dokumentā esošajai fotogrāfijai.
- 9.6. Datu subjektam ir tiesības saņemt tikai tos videonovērošanas datus, kuros ir redzams vai dzirdams konkrētais datu subjekts, kura vizuālais izskats sakrīt ar iesniegto fotogrāfiju un vizuālā izskata aprakstu. Videonovērošanas datus neizsniedz, ja negūst pietiekami pamatotu pārliecību par videonovērošanas datu pieprasīšanas pamatotību un datu subjekta atpazīstamību videomateriālā.
- 9.7. Datu subjektam nav tiesību saņemt videonovērošanas datus, kuros ir redzami vai dzirdami citi datu subjekti. Tāpēc datu subjektam izsniedz informāciju attiecībā uz videonovērošanu tikai noteiktajā veidā, bet neizsniedz videomateriāla kopijas rediģētā veidā, it īpaši tāpēc, ka atbilstoši Atbildīgās personas un Sabiedrības veiktās videonovērošanas apjomam, kontekstam un nolūkiem:
- 9.7.1. videonovērošanas vietā var atrasties citi datu subjekti, kuru dati nav izpaužami (ne identificētā, ne neidentificētā veidā);
- 9.7.2. rediģētā veidā sagatavotais videomateriāls var radīt maldīgu priekšstatu par patieso notikuma gaitu.
- 9.8. Datu subjektam neizsniedz informāciju attiecībā uz videonovērošanu, ja datu subjekta pieprasījums ir acīmredzami nepamatots (tai skaitā nesaistīts ar videonovērošanas nolūkiem vai ar nepietiekamu videonovērošanas datu pieprasīšanas pamatojumu), vai prasa pārmērīgas pūles, jo īpaši regulārās atkārtošanās dēļ.
- 9.9. Uz ikvienu datu subjekta rakstveida iesniegumu, tai skaitā par savu tiesību īstenošanu, Sabiedrība atbild datu subjektam viena mēneša laikā, izņemot normatīvajos aktos noteiktos datu subjektus, kuriem atbilde sniedzama īsākā laika periodā.
- 9.10. Ja datu subjekta tiesību īstenošana ir informācijas saņemšana attiecībā uz videonovērošanu, Atbildīgā persona pēc iespējas ņem vērā datu subjekta norādīto vēlamo videonovērošanas datu saņemšanas termiņu. Ja atbildi nav iespējams sniegt viena mēneša laikā vai citā normatīvajā aktā noteiktajā termiņā, datu subjekta sniedz starpatbildi, informējot par termiņu informācijas izsniegšanai.
- 9.11. Ja datu subjekts uzskata, ka videonovērošanas zonā ir noticis datu subjekta tiesību aizskārums, un ir nepieciešama steidzama pierādījumu nodrošināšana, datu subjekts ir tiesīgs vērsties tiesībsargājošā iestādē. Attiecīgi Sabiedrība šādā gadījumā sagatavo un sniedz informāciju uz šādu datu rezervācijas pieprasījumu.
- 9.12. Sabiedrība sadarbojas ar tiesībsargājošām iestādēm attiecībā uz jebkādas informācijas pieprasījumiem, kas apdraud personu vai sabiedrības drošību, datu apmaiņas procesu un, lai nodrošinātu tiesībsargājošām iestādēm nepieciešamās informācijas pieejamību.
- 10. Drošības incidentu izmeklēšanas kārtība**
- 10.1. Gadījumā, ja Sistēmas iekārta ir bojāta vai ir noticis nesankcionēts mēģinājums piekļūt informācijai, vai informācija, vai iekārtas daļa ir zudusi, tas uzskatāms par drošības incidentu.

- 10.2. Konstatējot personas datu aizsardzības pārkāpumu vai Sistēmas drošības incidentu, šo noteikumu pārkāpumu vai tā sekas, Atbildīgā persona veic šādas darbības:
- 10.2.1. pārbauda manuālos un elektroniskos auditācijas pierakstus un to integritāti piekļuvei Sistēmā un pārtrauc Sistēmas darbību, kamēr nav noskaidroti riski un incidenta cēloņi;
 - 10.2.2. pieprasa personas datu aizsardzības pārkāpumā vai drošības incidentā iesaistītajai personai rakstveida paskaidrojumu;
 - 10.2.3. par notikušo personas datu aizsardzības pārkāpumu vai iespējamo drošības incidenta esamību izdara ierakstu Pārkāpumu reģistrā (5.pielikums);
 - 10.2.4. noskaidro personas datu aizsardzības pārkāpuma vai drošības incidenta cēloņus un nepieciešamības gadījumā izstrādā grozījumus noteikumos, ieviešot papildu aizsardzības prasības;
 - 10.2.5. pieņem lēmumu par riska ietekmi uz datu subjekta tiesībām;
 - 10.2.6. ja personas datu aizsardzības pārkāpums vai drošības incidents var radīt risku datu subjekta tiesībām un brīvībām, tad Atbildīgā persona ziņo Sabiedrībai, kas par datu aizsardzības pārkāpumu nekavējoties paziņo Datu valsts inspekcijai un CERT.lv, bet ne vēlāk kā 72 stundu laikā no brīža, kad drošības incidents ir kļuvis zināms;
 - 10.2.7. ja konstatē, ka personas datu aizsardzības pārkāpums vai drošības incidents var radīt augstu risku datu subjekta tiesībām un brīvībām Sabiedrība nekavējoties par to paziņo datu subjektam;
 - 10.2.8. nepieciešamības gadījumā vainīgais darbinieks tiek saukts pie atbildības.
- 10.3. Ja rodas aizdomas par noziedzīgu nodarījumu (personas datu zādzība), Sabiedrība nekavējoties ziņo tiesībsargājošām iestādēm.
- 10.4. Sistēmas drošības incidentu gadījumā veic pārbaudi un nepieciešamības gadījumā ievieš citus drošības pasākumus.
- 10.5. Personas datu apstrādes aizsardzības drošības incidenta paziņojuma veidlapa Datu valsts inspekcijai ir pieejama:
<http://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/>.

11. Noslēguma jautājums

Noteikumos paredzētās drošības prasības pārskata vienu reizi gadā, kā arī, ja ir notikušas izmaiņas normatīvajos aktos.



TIEK VEIKTA VIDEONOVĒROŠANA

Mērķis: noziedzīgu nodarījumu novēršana un atklāšana, personu dzīvības, veselības un īpašuma aizsardzība, kā arī citu sabiedrības individu interešu ievērošanu un sabiedriskās kārtības nodrošināšana Duntē ielā 4. stāvā, Rīgā.

Pārzinis: SIA "Krassky", vienotais reģistrācijas Nr.540003774722, juridiskā adrese Duntē iela 3, Rīga.

Sīkāka informācija par datu subjekta tiesībām ir pieejama Pārziņa mājaslapā krassky.lv vai to var saņemt rakstot uz krassky@krassky.lv.

Nekustamā īpašuma Dunties ielā 3, Rīgā videonovērošanas sistēmas veikto videoierakstu (personas datu) apskates/nodošanas trešajām personām reģistrācijas lapa Nr.1

Nr. p.k.	Datums un laiks	Trešā persona, vārds, uzvārds, amats, kura piedalījās datu apskatē	Trešās personas paraksts vai nosūtīšanas adrese	Atbildīgās personas paraksts	Ieraksta apskates /nodošanas iemesls	Datums un laiks par kādu periodu tika veikta ieraksta apskate/nodošana
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Nekustamā īpašuma Dunties ielā 3, Rīgā videonovērošanas sistēmas veikto videoierakstu (personas datu) kopēšanas uz citiem datu nesējiem reģistrācijas lapa Nr.2

Nr. p.k.	Datums un laiks	Vārds, uzvārds, amats, kura piedalījās datu kopēšanā	Atbildīgās personas paraksts	Ieraksta kopēšanas iemesls	Datums un laiks par kādu periodu tika veikt ieraksts kopēšana
1.					
2.					
3.					
4.					
5.					
6.					
7.					

4. pielikums
Videonovērošanas sistēmas drošības noteikumiem

Nekustamā īpašuma Dunties ielā 3, Rīgā videonovērošanas sistēmas veikto videoierakstu (personas datu) dzēšanas reģistrācijas lapa Nr.3.

Nr. p. k.	Datums un laiks	Vārds, uzvārds, amats, kura piedalījās datu dzēšanā	Atbildīgās personas paraksts	Ieraksta dzēšanas iemesls	Datums un laiks par kādu periodu tika veikta ieraksta dzēšana
1.					
2.					
3.					
4.					
5.					
6.					
7.					

5. pielikums
Videonovērošanas sistēmas drošības noteikumiem

Pārkāpumu (incidentu) reģistrs

Nr.	Pārzinis	Iesaistītais apstrādātājs	Incidents (raksturojums)	Datums	Ietekme	Pārvaldība	Incidenta nozīmīgums