|  |
| --- |
| ectaalogo-new  Ref: BC18-013-4477 |

**Biežāk uzdotie jautājumi par Vispārīgo datu aizsardzības regulu**

## Vispārīga datu aizsardzības regula (VDAR) - klientu datu apstrāde

**Atruna:** Šis pārskats ir paredzēts, lai sniegtu VDAR vispārējās vadlīnijas ceļojumu aģentūrām un tūrisma operatoriem, un tās nevar uzskatīt par galīgiem ieteikumiem konkrētajās situācijās. Katras dalībvalsts uzraudzības iestādes sniegs norādes par īpašajām prasībām katrā jurisdikcijā. **Šaubu gadījumā ieteicams vērsties savā uzraudzības iestādē, lai saņemtu papildu norādījumus.**

## SATURS:

## [Pārskats](#_Overview)

## [Datu pārzinis un datu apstrādātājs](#_Data_controller_and)

## [Datu aizsardzības speciālists](#_Data_Protection_Officer)

## [Personu tiesības](#_Individuals’_Rights)

## [Datu apstrādes juridiskais pamats](#_Legal_Basis_for)

## [Piekrišana](#_Consent)

## [Paziņojumi par personas datu aizsardzību](#_Privacy_Notices)

## [Starptautiskie pārskaitījumi](#_International_Transfers)

## [Tiešais mārketings](#_Direct_Marketing)

## [Drošība](#_Security)

### Pārskats

**Kas ir VDAR?**

VDAR ir Eiropas Parlamenta un Padomes Regula ([Regula (ES) 2016/679](https://ec.europa.eu/info/files/regulation-eu-2016-679-protection-natural-persons-regard-processing-personal-data-and-free-movement-such-data_en) ) ar ko nosaka jaunus noteikumus par to, kā rīkoties ar personas datiem. Šī regula ir īpaši svarīga tūrisma nozarē, jo uzņēmumi, piemēram, ceļojumu aģentūras un tūroperatori, katru dienu apstrādā klientu datus (piemēram, veicot rezervācijas, mārketinga aktivitātēs). Regulas prasības būs piemērojamas, sākot ar 2018. gada 25. maiju

Regula attiecas uz **personas datu apstrādi**. **Personas datu apstrāde** ir jebkura darbība, kas veikta ar datiem, piemēram, datu vākšana, uzglabāšana, reģistrēšana, izmantošana vai koplietošana, izmantojot gan automatizētu, gan manuālu apstrādi.

Jāuzsver, ka regula attiecas uz visiem datiem, ne tikai uz klientu datiem, tāpēc ieteicams pārskatīt veiktos procesus attiecībā uz personālu, kā arī uz citiem uzņēmuma rīcībā esošiem datiem. Taču šis pārskats ir paredzēts, lai atbildētu uz visbiežāk uzdotajiem jautājumiem par klientu datiem.

**Kā tiks ietekmēta uzņēmējdarbība?**

Apstrādājot klientu personas datus, jāievēro vairākas prasības, kas var ietekmēt ierasto darba procesu, piemēram:

*1. Darbinieku informētība*

Jāveicina izpratne par VDAR radītajām izmaiņām darbinieku vidū. Visiem darbiniekiem jāpārzina regulas ietekme un jānosaka jomas, kas varētu radīt atbilstības problēmas VDAR. Datu aizsardzība jāiekļauj uzņēmuma riska reģistrā. *Kā iepriekš norādīts, jāņem vērā arī datu apstrādes procesi saistībā ar uzņēmuma rīcībā esošajiem datiem par personālu*.

*2. Informācijas pārvaldība*

Ieteicams dokumentēt, kādi personiskie dati ir savākti, datu avots, kādā nolūkā un cik ilgi dati tiks uzglabāti un kopīgoti. Šim mērķim jāorganizē informācijas audits visā organizācijā vai konkrētā darbības jomā.

*3. Privātuma politikas pārskatīšana*

Ieteicams pārskatīt pašreizējos paziņojumus par konfidencialitāti un veikt nepieciešamās izmaiņas VDAR atbilstībai. VDAR nosaka, lai informācija tiktu sniegta saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu.

*4. Personas tiesības*

Jāpārskata procedūras, nodrošinot, ka tiek ievērotas visas klientiem pieškirtās tiesības saskaņā ar VDAR. [*Skat. turpmāk*](#_Legal_Basis_for)

*5. Subjekta piekļuves pieprasījumi*

Jāizlemj, kā tiks apstrādāti pieprasījumi viena mēneša laikā un sniegta jebkāda papildu informācija. Ir pamats atteikties no subjekta piekļuves pieprasījuma ievērošanas - par acīmredzami nepamatotiem vai pārmērīgiem pieprasījumiem var piemērot samaksu vai atteikumu. Jāizveido sistēma, lai risinātu citus klientu pieprasījumus, piemēram, tiesības labot neprecīzus datus. Būtu lietderīgi apsvērt iespēju izveidot sistēmas, kas personām ļautu piekļūt savai informācijai tiešsaistē.

*6. Datu apstrādes juridiskais pamats*

Jāizskata dažādi datu apstrādes veidi, jānosaka juridiskais pamats procesa veikšanai, un to ieteicams dokumentēt. [*Skat. turpmāk*](#_Legal_Basis_for)

*7. Piekrišana*

Ja par datu apstrādes juridisko pamatu tiek izmantota piekrišana (un tas ir nepieciešams, apstrādājot īpašās kategorijas datus), no klienta ir jāsaņem nepārprotama piekrišana datu savākšanai un apstrādāšanai. [*Skat. turpmāk*](#_Consent)

*8. Īpašas kategorijas dati*

Īpašas kategorijas datus, piemēram, informāciju par klienta rasi vai etnisko izcelsmi, reliģisko pārliecību, veselību, invaliditāti vai seksuālo orientāciju, var apstrādāt tik ilgi, cik tas ir nepieciešams, lai veiktu rezervāciju, un ar nosacījumu, ka ir saņemta klienta nepārprotama piekrišana.

*9. Datu aizsardzības pārkāpumi*

Jāpārliecinās, ka ir piemērotas procedūras, lai atklātu, ziņotu un izmeklētu personas datu pārkāpumu. Tas ietvert esošo datu veidu novērtēšanu un datu dokumentēšanu, par kuriem jāziņo datu aizsardzības pārkāpuma gadījumā. Dažos gadījumos ir jāziņo klientiem, kuru dati ir tieši pakļauti pārkāpumam, piemēram, ja pārkāpums varētu viņus pakļaut iespējamiem finansiāliem zaudējumiem. Lielākām organizācijām jāizstrādā politika un procedūras datu pārkāpumu pārvaldīšanai - gan visa uzņēmuma, gan struktūrvienību līmenī. Jāatzīmē, ka par prasības neievērošanu un neziņošanu par pārkāpumu var piemērot naudas sodu.

*10. Starptautiskie pārskaitījumi*

Jānodrošina juridisks pamats personas datu pārsūtīšanai jurisdikcijām, kuras nav atzītas par atbilstošām datu aizsardzības noteikumiem. Parasti šādā gadījumā ir nepieciešama datu subjekta piekrišana, it īpaši, ja dati iekaļauj pases informāciju un informāciju par veselību un uztura ierobežojumiem. [*Skat. turpmāk*](#_International_Transfers)

*11. Datu aizsardzības procesu dokumentēšana*

Jāuzsver, ka datu aizsardzības procesi un procedūras ir jāreģistrē. Tas palīdzēs, ja būs jautājumi par jebkuru datu pārvaldības aspektu. Ieteicams dokumentēt lēmumus par datu aizsardzības speciālista iecelšanu; jebkādu datu vākšanas ietekmes novērtējumu; jebkuru novērtējumu par spēju pamatoties uz leģitīmu interešu pamatu datu apstrādei; un piekrišanu, kas iegūta no datu subjektiem.

*12. Cik ilgi jāglabā klientu personas dati?*

VDAR nav skaidri noteikts termiņš. VDAR nosaka, ka "personas datus uzglabā ne ilgāk, kā tas ir nepieciešams mērķiem, kuriem dati tiek apstrādāti". Konkrētiem datiem piemēro valsts tiesībās noteiktos noilguma termiņus un citus likumā noteiktos termiņus, tādēļ ir svarīga droša datu glabāšana, lai tie būtu pieejami šiem mērķiem. Tomēr iespējams, ka liela daļa rezervācijas datu (piemēram, pases un maksājuma informācija) nebūs vajadzīgi tiesvedības uzsākšanai vai sūdzību izskatīšanai, un, ja iespējams, šie dati jāiznīcina, tiklīdz tie nav nepieciešami.

*13. Kādi ir riski, ja nav atbilstība jaunajiem VDAR noteikumiem?*

Neievērošanas sekas varētu būt nopietnas. Neizpildot VDAR noteikumus, var tikt uzlikts naudas sods līdz 4% no gada apgrozījuma vai 20 miljoni EUR, atkarībā no tā, kura summa ir lielāka.

### Datu pārzinis un datu apstrādātājs

Atbilstoši VDAR, datu apstrādes procesu palīdz veikt datu pārzinis un datu apstrādātājs.

### Kas ir datu pārzinis? Kas ir datu apstrādātājs? Kāds ir ceļojumu aģentūras vai tūroperatora uzdevums?

* Datu pārzinis nosaka, kādā veidā un kādiem mērķiem tiek apstrādāti personas dati. Tas varētu būt ceļojumu aģentūras vai tūroperatora pienākums. Datu pārzinis var izmantot citus uzņēmumus, lai veiktu apstrādes pakalpojumus. Šādā gadījumā datu pārzinis ir atbildīgs par datu apstrādi.
* Datu apstrādātāji ir personas, kas apstrādā datus pārziņa vārdā. VDAR nosaka, ka datu apstradātāji arī ir atbildīgi par pārkāpumiem vai neatbilstību. Iespējams, ka gan uzņēmums, gan datu apstrādes partneris būs atbildīgs par sodu, pat ja vaina pilnībā attiecas uz apstrādes partneri.
* Ceļojumu aģentūra vai tūroperators, atkarībā no situācijas, var būt gan datu pārzinis, gan datu apstrādātājs. Ceļojumu aģentūra vai tūroperators, kas tieši sazinās ar klientiem, visticamāk, būs datu pārzinis.

**Ko darīt ar datiem, kas nosūtīti tirdzniecības partneriem, piemēram, aviosabiedrībām un viesnīcām?**

Darījumu partneris var būt arī datu pārzinis, jo VDAR paredz tādu iespēju. Tādēļ uzņēmumam jānoformē attiecības ar saviem biznesa partneriem:

* iepriekš jānosaka, kāda veida attiecības uzņēmumam būs ar biznesa partneriem attiecībā uz personas datu apstrādi,
* jāinformē klienti par to, ka viņu datus apstrādās trešās personas, un jānorāda trešo personu identitāte paziņojumā par personas datu aizsardzību.
* GDS tiek uzskatīta par datu pārzini CRS rīcības kodeksa mērķiem, taču darbosies arī kā datu apstrādātājs citiem datu apstrādes mērķiem.

## Datu aizsardzības speciālists

## Kas ir datu aizsardzībasspeciālists?

Datu aizsardzības speciālists ir atbildīgs par datu aizsardzības stratēģijas un īstenošanas uzraudzību, nodrošinot atbilstību VDAR prasībām.

### Vai uzņēmumam ir nepieciešams datu aizsardzības speciālists?

Pienākums un nosacījumi datu aizsardzības speciālista iecelšanai ir atkarīgi no valsts, kurā uzņēmums ir reģistrēts, un atbilstošiem valsts tiesību aktiem **(aizpilda ECTAA dalībnieks, atbilstoši attiecīgās valsts nosacījumiem)**. Tomēr, pat ja tas nav obligāti, visiem uzņēmumiem ir ieteicams apsvērt, vai viņiem ir vai nav jāieceļ datu aizsardzības speciālists, un, ja tiek nolemts to nepieaicināt, vajadzētu pierakstīt minētā lēmuma iemeslus, lai tie, vajadzības gadījumā, būtu pieejami ziņojumam attiecīgajai uzraudzības iestādei.

## 

## Personas tiesības

Galvenās tiesības indivīdiem saskaņā ar VDAR ir:

• tiesības zināt, ka viņu dati tiek apstrādāti;

• piekļūt saviem personas datiem.

Par šo informāciju nevarat ņemt maksu, un šī informācija jāsniedz mēneša laikā pēc pieprasījuma saņemšanas.

Turklāt klientiem ir tiesības labot personas datus, ja tie ir neprecīzi vai nepilnīgi.

Klienti var pieprasīt arī personas datu dzēšanu vai iznīcināšanu, ja nav pārliecinošu iemeslu datu apstrādes turpināšanai (zināmas kā tiesības uz dzēšanu vai tiesības tikt aizmirstam). Tas attiecas uz gadījumiem, kad:

* personas dati vairs nav vajadzīgi mērķim, kuram tie sākotnēji tika savākti vai apstrādāti;
* uzņēmums ir paļāvies uz piekrišanu kā likumīgo pamatu datu glabāšanai, un persona atsauc savu piekrišanu;
* uzņēmums ir paļāvies uz leģitīmām interesēm datu apstrādes pamatā, bet persona iebilst pret datu apstrādi, un nepastāv primāras leģitīmas intereses turpināt šo apstrādi;
* personas dati tiek apstrādāti tiešā mārketinga nolūkos, un persona iebilst pret šo apstrādi;
* personas dati tiek apstrādāti bez atbilstoša juridiskā pamata;
* personas dati tiek apstrādāti, lai izpildītu juridiskas saistības; vai
* personas dati tiek apstrādāti, lai piedāvātu pakalpojumus tiešsaistē (Informācijas sabiedrības pakalpojumi) bērnam.

Tiesības dzēst nav spēkā, ja apstrāde ir nepieciešama kāda turpmāk minētā iemesla dēļ:

* izmantot tiesības uz vārda un informācijas brīvību;
* lai izpildītu juridiskas saistības;
* juridisko prasību izveidošanai, īstenošanai vai aizstāvībai.

Pastāv tiesības uz datu pārnesamību, ja klients pieprasa, lai personas dati tiktu iesniegti citam datu pārzinim. To piemēro, ja apstrādi veic automātiski, balstoties uz piekrišanu, vai tāpēc, ka apstrāde ir nepieciešama līguma izpildei un klients ir sniedzis datu pārzinim datus. "Datu sniegšana" ietver datus, kas iegūti, novērojot klienta darbību, piemēram, pagātnes rezervācijas un izdevumus.

Šīs tiesības ļauj klientiem iegūt un atkārtoti izmantot savus personas datus saviem nolūkiem dažādu pakalpojumu saņemšanai. Tas ļauj viegli un drošā veidā pārvietot, kopēt vai pārsūtīt personas datus no vienas IT vides uz otru. Informācija jāsniedz strukturētā, vispārpieņemtā un mašīnlasāmā formātā, kuru var viegli pārsūtīt citam datu pārzinim, un uzņēmums par to nevar ņemt maksu.

## Datu apstrādes juridiskais pamats

Personas datu apstrādei ir nepieciešams juridisks pamats. Juridiskajam pamatam datu apstrādei ir jābūt kādam no turpmāk minētajiem:

1. piekrišana datu apstrādei, kas saņemta no personas vai, ja tas ir bērns, no viņu vecāka vai aizbildņa; vai

2. apstrāde ir nepieciešama saistībā ar līgumu, kuru persona ir noslēgusi brīvdienās vai citā kārtībā, vai tāpēc, ka persona ir lūgusi kaut ko darīt, lai varētu noslēgt līgumu; vai

3. dati jāapstrādā juridiskā pienākuma dēļ, kas attiecas uz uzņēmumu (nevis saskaņā ar līgumu); vai

4. apstrāde notiek saskaņā ar leģitīmo interešu nosacījumu (tas tiek interpretēts sašaurināti, tāpēc to nevar izmantot, lai vienkārši aprakstītu parastās uzņēmējdarbības intereses, un uzņēmumam, iespējams, vajadzēs ignorēt citu juridisko pamatu nepieciešamību).

### 

### **Leģitīmās intereses novērtējums**

Lai varētu paļauties uz datu apstrādes iemeslu, jāspēj pierādīt, ka tiek piemērotas noteiktas prasības (t.i., jāveic leģitīmo interešu novērtējums):

1. Pirmā prasība ir tāda, ka jāapstrādā informācija par uzņēmuma leģitīmo interešu nolūkiem vai trešās puses vajadzībām, kurām tā tiek izpausta. VDAR nosaka, ka personas datu apstrādi tiešā mārketinga nolūkos var uzskatīt par tādu, kas tiek veikta leģitīmo interešu nolūkā (uzmanīgi ar e-mārketingu).

2. Otrā prasība ir tā, ka leģitīmām interesēm jābūt līdzvērtīgām attiecīgās personas (-u) interesēm.

3. Visbeidzot, informācijas apstrādei saskaņā ar leģitīmo interešu prasībām jābūt godīgai un likumīgai, un tai jāatbilst visiem datu aizsardzības principiem, piemēram, pārredzamībai, precizitātei, atbilstībai un drošībai.

### Piekrišana

Saskaņā ar VDAR piekrišana izpaužas kā nepārprotama, skaidra rīcība.

Piekrišanai jābūt:

* **Nepārprotamai**: Piekrišanai nepieciešams vai nu paziņojums, vai skaidri apstiprinoša darbība, lai tā būtu derīga (piem., atzīmējot lodziņu). Klusēšana, iepriekš atzīmēti laukumi vai atturēšanās no darbības tādējādi nebūtu jāuzskata par piekrišanu.
* **Brīvi dotai**: Vajadzētu būt iespējai atteikties. Piemēram, nevar uzstāt, ka rezervācija tiks pabeigta tikai tad, kad klients piekritīs jaunumu saņemšanai / mārketinga korespondencei.
* **Konkrētai:** Piekrišanai jābūt saistītai ar konkrētām datu apstrādes darbībām (piemēram, lidojuma rezervēšana, mārketinga mērķi). Tādējādi vispārēja plaša piekrišana nenoteiktām apstrādes darbībām būs nederīga.
* **Atteikuma tiesības**: Klientam jebkurā laikā jābūt iespējai atteikties. Tādēļ, ja tas vēl nav izdarīts, jāapsvēr iespējas "atrakstīties " pievienošana sarakstē un tīmekļa vietnē.
* **Formālai**: Jebkurā laikā jāspēj pierādīt, ka no klienta ir saņemta nepārprotama piekrišana. Jebkurš rakstisks pierādījums ir derīgs. Ir iespējams saņemt mutisku piekrišanu (pa tālruni), lai gan tas būs uzņēmuma - kā datu pārziņa - ziņā, pierādot piekrišanas saņemšanu (piemēram, ierakstot tālruņa sarunu).

Tāpēc ieteicams pārbaudīt uzņēmuma iekšējos procesus un pārliecināties par iepriekš minēto nosacījumu izpildi. Pretējā gadījumā attiecīgi jāmaina darba metodes.

**Vai tā tiek uzskatīta par piekrišanu, ja netiek dota atbilde?**

Nē, tā netiek uzskatīta par nepārprotamu piekrišanu un nevajadzētu izmantot klienta datus.

**Kā saņemt piekrišanu, organizējot skolas braucienu?**

Ja tiek organizēti skolas braucieni, jāpārliecinās, ka nepilngadīgā vecāki / skolotāji ir pienācīgi informēti, ka bērnu dati tiks izmantoti brauciena organizēšanā. Atbildīgajam skolotājam vai darbiniekam jāsaņem atļauja no vecākiem, lai apkopotu nepilngadīgo bērnu datus un pārsūtītu tos brauciena organizētājam. Tas nozīmē, ka vecāku parakstītajā veidlapā jāiekļauj paziņojums par konfidencialitāti, informējot viņus par iepriekš minēto. No vecākiem jāsaņem piekrišana par to, ka skolotājs drīkst savākt bērnu datus, nodot tos ceļojumu aģentūrai un pēc tam nodot ceļojumu pakalpojumu sniedzējiem. Būtu ieteicams sagatavot parauga veidlapu, kuru paraksta vecāki / pasniedzēji.

**Paziņojums par personas datu aizsardzību**

**Kas jāiekļauj paziņojumā?**

Privātpersonām ir tiesības tikt informētām par to, ka viņu dati tiek apstrādāti. Šo informāciju vajadzētu sniegt, izmantojot paziņojumus par personas datu aizsardzību. Ir saraksts ar informāciju, kas jāiekļauj paziņojumā par personas datu aizsardzību, un tā jāsniedz īsā, pārredzamā, saprotamā un viegli pieejamā veidā, skaidrā un vienkāršā valodā, un bez maksas.

Līdztekus paziņojumam par personas datu aizsardzību jānodrošina, ka klienti tiek informēti ikreiz, kad tiek veikta datu vākšana, norādot iemeslu un kādam nolūkam dati tiks izmantoti. Ja ir jāsaņem klienta piekrišana datu apstrādei, piemēram, ja piegādātājam jānosūta īpašas kategorijas dati, klients noteikti jāinformē, ar ko šie dati tiks koplietoti.

Saite uz uzņēmuma paziņojumu par personas datu aizsardzību jānorāda rezervēšanas procesa sākumposmā.

Paziņojumā par personas datu aizsardzību jāiekļauj šāda informācija:

Ja dati ir savākti tieši no datu subjekta, jānorāda:

* Datu pārziņa vai datu pārziņa pārstāvja identitāte un kontaktinformācija.
* Datu aizsardzības speciālista kontaktinformācija, ja tāds ir iecelts.
* Datu apstrādes iemesls un juridiskais pamats.
* Leģitīmās intereses, ja uzņēmums paļaujas uz leģitīmo interešu nosacījumiem.
* Ar ko dati tiks koplietoti. Tas būs piegādātāju saraksts, ja iespējams, vai piegādātāju kategorijas, piemēram, aviosabiedrības, viesnīcas utt.
* Ja koplietošana un turpmākā datu izmantošana pamatojas uz piekrišanu, datu subjekti jāinformē par personas datu apstrādātāju identitāti, kuri apstrādās datus, pamatojoties uz šo piekrišanu.
* Gadījumos, kad dati tiek nosūtīti ārpus EEZ, kādi drošības pasākumi ir spēkā.
* Datu glabāšanas laikposms vai kritēriji, pēc kuriem tiek noteikts glabāšanas periods.
* Norāde, ka datu subjektam ir tiesības pieprasīt piekļuvi saviem datiem, kļūdu labošanai, datu dzēšanai, kā arī tiesības uz datu pārnesamību.
* Tiesības atsaukt piekrišanu, ja datu apstrāde notiek, pamatojoties uz subjekta piekrišanu.
* Datu subjekta tiesības iesniegt sūdzību attiecīgajai uzraudzības iestādei.
* Tas, vai personas datu sniegšana ir daļa no tiesību aktos vai līgumā noteiktajām prasībām vai pienākumiem, un iespējamās sekas, ja personas dati netiek sniegti.

Ja dati nav saņemti tieši no datu subjekta, jāsniedz šāda papildu informācija:

* Uzņēmuma rīcībā esošās personas datu kategorijas. Vajadzētu paskaidrot, kādi dati tiek izmantoti, ja indivīdi paši tos nav norādījuši.
* Datu ieguves avots.

**Kur jāizvieto paziņojums par personas datu aizsardzību un kurā rezervācijas procesa posmā tas jādara?**

Klienti jāinformē par datu vākšanu un izmantošanu visa rezervēšanas procesa gaitā. Šī informācija jānorāda papildus paziņojumam par personas datu aizsardzību.

Kā daļa no rezervēšanas procesa, kas notiek tiešsaistē vai bezsaistē, veikalā vai pa tālruni, jāiesniedz paziņojums, līdzīgs šim:

Mēs apkopojam jūsu personīgo informāciju, lai rezervētu pieprasītos ceļojumu pakalpojumus. Šī informācija, ieskaitot jebkādu informāciju par jebkādiem veselības vai medicīniskiem jautājumiem, par ko jūs mūs informējat, un jūsu pases dati tiks nosūtīti piegādātājiem, kuri sniegs ceļojuma pakalpojumus. Šie piegādātāji var būt ārpus ES, kur personas datu aizsardzība var nebūt tik spēcīga.

*Parakstot šo rezervācijas veidlapu / atzīmējot šo izvēles rūtiņu / dodot piekrišanu*, jūs piekrītat, ka jūsu personas dati tiks nosūtīti rezervācijas nolūkos. Ar uzņēmuma paziņojumu par personas datu aizsardzību var iepazīties tīmekļa vietnē.

Jūsu dati tiks izmantoti, lai informētu jūs par ceļojumu piedāvājumiem, kas, mūsuprāt, varētu jūs interesēt. *Atzīmējiet šeit / norādiet*, ja nevēlaties saņemt šādus piedāvājumus.

Attiecībā uz pārdošanu pa tālruni rīcības plānā varētu iekļaut ierakstītu ziņojumu, kas tiks atskaņots, klientam sazinoties ar zvanu centru. Piekrišana jāsaņem e-pastā vai janosūta pa pastu pēc sarunas.

### Starptautiskie pārskaitījumi

Ceļojumu aģentūras un tūroperatori sadarbojas ar tirdzniecības partneriem, kas nav reģistrēti ES / EEZ. Tādēļ ir svarīgi precizēt attiecības ar šiem partneriem. Uzņēmumam vajadzētu nodrošināt atbilstošu juridisko pamatu personas datu pārsūtīšanai, lai nepieciešamības gadījumā būtu iespējams pārsūtīt datus uz valstīm, kuras nenodrošina pienācīgu aizsardzības līmeni, kā to nosaka Komisija. *Rakstīšanas brīdī tikai šādām valstīm ārpus EEZ ir nodrošināta pietiekama aizsardzības pakāpe: Andora, Argentīna, Farēru salas, Gērnsija, Menas sala, Izraēla, Džērsija, Jaunzēlande, Šveice un Urugvaja. Tiek uzskatīts, ka arī Kanādai un ASV ir pietiekams aizsardzības līmenis ierobežotos gadījumos.*

Ja regulāri tiek pārsūtīti dati piegādātājam vai citam partnerim, kas atrodas valstī, kurai nav atbilstoša aizsardzības līmeņa, jāpārliecinās, ka ir ieviesti atbilstoši aizsardzības pasākumi. To var nokārtot, iekļaujot līgumā ar piegādātāju standarta datu aizsardzības klauzulas, ko pieņēmusi Komisija vai uzraudzības iestāde. Eiropas Komisija līdz šim ir izdevusi divas standarta līguma klauzulas par datu pārsūtīšanu no ES datu pārziņiem tiem datu pārziņiem, kas reģistrēti ārpus ES vai Eiropas Ekonomikas zonas (EEZ). ES ir arī izdevusi vienu līgumu klauzulu kopumu datu pārsūtīšanai no datu pārziņiem ES tiem pārziņiem, kas reģistrēti ārpus ES vai EEZ <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en>

Ja datu pārsūtīšana nav regulārs process, datus var pārsūtīt, pamatojoties uz nepieciešamību pārsūtīt datus par līguma izpildi vai, ja ir iesaistīti īpašas kategorijas dati, pamatojoties uz datu subjekta piekrišanu. Ceļojuma aģentūras individuālo klientu datu pārsūtīšanu viesnīcām vai citiem komerciālajiem partneriem, kas tiek pieprasīti, organizējot šo klientu uzturēšanos ārzemēs, 2018. gada 6. februāra 29. panta darba grupas dokumentā tika minēts kā piemērs, kad varētu notikt neregulāras pārsūtīšanas kārtība.

### Tiešais mārketings

**Vai savāktie dati var tikt izmantoti tiešā mārketinga veikšanai?**

VDAR izpratnē atbilstošos apstākļos iespējams izmantot leģitīmās intereses kā juridisko pamatu datu apstrādei tiešā mārketinga nolūkos. Ieteicams veikt leģitīmas intereses novērtējumu ([***skatīt iepriekš***](#_Legitimate_Interest_Assessment)), bet, ja mārketinga aktivitates iekļauj tikai ceļojumu pakalpojumus un datu subjektam ir skaidri izklāstīts, kā atteikties no turpmākām mārketinga aktivitātēm, visticamāk, ka šādam novērtējumam vajadzētu norādīt vajadzīgo interešu līdzsvaru.

Attiecībā uz elektronisko mārketingu tiek piemēroti e-privātuma direktīvas noteikumi, kas nozīmē, ka individuālo personu dati, tostarp individuālā komersanta vai partnerattiecību uzņēmumu darbinieku dati (atšķirībā no sabiedrību ar ierobežotu atbildību un PLC darbinieku datim), var tikt izmantoti tikai tiešā mārketinga nolūkos, ja datu subjekti ir devuši piekrišanu.

Tomēr e-mārketingu var veikt arī tādā veidā, ko sauc par "soft opt-in" izvēli, ja:

1. dati ir iegūti no datu subjekta, izmantojot iepriekšējo uzņēmuma pakalpojumu pārdošanu; un
2. ja datu subjektam tika dota iespēja atteikties no uzņēmuma mārketinga informācijas saņemšanas un tā netika izmantota; un
3. ja mārketinga aktivitātes attiecas uz līdzīgiem pakalpojumiem, par kuriem datu subjekts iepriekš ir izrādījis interesi; un
4. ja klientam ir dota iespēja bez maksas un viegli atteikties no šādas elektroniskās kontaktinformācijas izmantošanas katra nākamā ziņojuma saņemšanas gadījumā.

**Kā rīkoties ar veco e-pasta adrešu datu bāzi?**

Vispirms tas ir atkarīgs no tā, kā tika savākti dati. Ja dati tika savākti pārdošanas vai pārrunu laikā par pakalpojumu pārdošanu un datu subjektiem tika dota iespēja atteikties no turpmākiem sūtījumiem un tā netika izmantota, ir iespēja turpināt izmantot šos datus saskaņā ar e-privātuma direktīvu un pamatojoties uz leģitīmo interesi, kā nosaka GDPR.

**Kā rīkoties ar kontaktu sarakstu, kas iegūts no citiem tirgotājiem vai specializētiem uzņēmumiem?**

Ievērojot valstu tiesību aktus, var izmantot sarakstus, kas iegūti no citiem tirdzniecības partneriem, ja sarakstā iekļautās personas ir devušas nepārprotamu piekrišanu, apzinās tirgotaja identitāti un kādā nolūkā dati tiek savākti.

**Kas rīkoties pasākumos, kad viesi / apmeklētāji dod vizītkartes vai piedalās konkursos, sniedzot personisko informāciju (piemēram, e-pasta adresi)?**

Ja uzņēmums organizē pasākumu, lai savāktu e-pastus, ir iespējams izmantot datus, kas apkopoti saskaņā ar VDAR. Vajadzētu skaidri noteikt, kādi dati tiks savākti. Ja tos paredzēts izmantot citiem mērķiem, kas nav konkurss (piemēram, mārketings), tad, saskaņā ar VDAR, varētu atsaukties uz leģitīmām interesēm kā datu apstrādes juridisko pamatu. Tomēr, ja mārketinga aktivitātes jāveic elektroniski, tad jāpiemēro e-privātuma direktīvas noteikumi, un datu subjektu piekrišana ir nepieciešama, ja tie ir personīgie abonenti.

Grūti nošķirt datus, kas savākti no personīgajiem un korporatīvajiem abonentiem, tāpēc ieteicams visus datu subjektus uzskatīt par personīgiem abonentiem. Piekrišanu varētu saņemt datu savākšanas laikā vai, ja to pieļauj valsts tiesību akti, nosūtot papildu e-pastu bez mārketinga satura, izsakot vēlmi saņemt piekrišanu tālākai e-pastu sūtīšanai mārketinga nolūkos.

**Vai vajadzētu veikt īpašus piesardzības pasākumus, izmantojot mārketinga nolūkos klientu fotogrāfijas?**

Ja fotogrāfijas tiek izmantotas mārketinga mērķiem (brošūra, tīmekļavietne, plašsaziņas līdzekļi), kas ietver indivīdus, ir jāsaņem nepārprotama rakstiskā piekrišana no visiem attēlā redzamajiem.

Labākais veids, kā to panākt, ir fotogrāfijas izmantošanas veidlapa. Tai jābūt parakstītai, un skaidri jānorāda, kā fotogrāfija tiks izmantota. Ja fotogrāfijā ir bērni, kas jaunāki par 18 gadiem, jāsniedz rakstiska vecāku piekrišana.

Jāuzsver, ka pat pēc tam, kad ir saņemta nepārprotama piekrišana, fotogrāfijās attēlotajiem indivīdiem vienmēr ir:

* Tiesības būt informētiem: skaidri jāinformē par fotogrāfijas izmantošanas kontekstu (piemēram, plašsaziņas līdzekļi, tīmekļa vietnes, brošūras). Tas arī nozīmē, ka nevajadzētu izmantot fotogrāfiju mērķim, par kuru iepriekš nebija panākta vienošanās.
* Piekļuves tiesības: privātpersonām ir tiesības piekļūt saviem personas datiem (fotogrāfijām) pēc pieprasījuma un saņemt apstiprinājumu par to, kā tās tiek izmantotas.
* Tiesības tikt aizmirstam / tiesības uz dzēšanu: privātpersonām ir tiesības pieprasīt, lai fotogrāfijas tiktu izņemtas no tīmekļa vietnēm, plašsaziņas līdzekļiem un / vai drukāto materiālu nākotnes versijām.

Tādēļ ir ieteicams sekot līdzi:

* kā un kādam nolūkam fotogrāfijas tiek izmantotas,
* kas ir personas, kas identificējamas uz fotogrāfijas,
* kur tiek uzglabātas fotogrāfijas un fotogrāfiju izmantošanas veidlapas.

**Cik ilgi jāglabā klientu personas dati?**

VDAR nav skaidri noteikts termiņš. VDAR norāda, ka "personas dati netiek uzglabāti ilgāk, kā tas ir nepieciešams mērķiem, kuriem tie tiek apstrādāti". Tiešā mārketinga nolūkos, ja tas balstās uz leģitīmām interesēm un „soft opt-in“ izvēli saskaņā ar e-privātuma Direktīvu, un skaidri norāda, kā atteikties no turpmākiem sūtījumiem, datus var izmantot, ja vēstkopas tiek sūtītas regulāri. Ja vēstkopas nav sūtītas ilgāk par 12 mēnešiem, tad nepietiks ar „soft opt-in“ izvēli vai leģitīmo interešu pamatu. Parasti uzņēmumi vēlas saglabāt individuāļu datus, kuri nav reaģējuši uz vēstkopām ilgāk par 24 mēnešiem, nosūtot e-pastu un lūdzot viņiem atjaunināt informāciju un apstiprināt, ka viņi piekrīt turpmākiem sūtījumiem.

## Drošība

**Kādi pasākumi jāveic, lai izpildītu VDAR drošības prasības:**

Ieteicams veikt detalizētu un objektīvu uzņēmuma rīcībā esošo datu pārbaudi - kur šie dati tiek uzglabāti, ar ko kopīgoti un kādiem mērķiem glabāti. Jāveic novērtējums, kurā norādīts apstrādājamo personas datu veids, apstrādes darbības un novērtēti riski.

Balstoties uz novērtējumu, jāievieš atbilstoši tehniskie un organizatoriskie pasākumi:

* Personas datu pseidonimizācija un šifrēšana.
* Apstrādes sistēmu un pakalpojumu pastāvīgas konfidencialitātes, integritātes, pieejamības un noturības nodrošināšana (piemēram, spēcīga parole, programmatūras regulāra atjaunināšana un aizsardzība, pretvīrusu un destruktīva programmatūra).
* Pieejamības un piekļuves atjaunošana personas datiem fiziska vai tehniska rakstura notikuma gadījumā (piemēram, regulāra dublēšana).
* Tehnisko un organizatorisko pasākumu regulāras testēšana un novērtēšana, lai nodrošinātu apstrādes drošību.
* Personāla, uzņēmēju, pārdevēju un piegādātāju pastāvīga pārbaude un apmācība.
* Personāla apmācība datu apstrādes pienākumu veikšanā, pārkāpumu un risku noteikšanā. Pat mūsdienīgākā drošības programmatūra nevarēs novērst dažus pārkāpumus bez pienācīgi apmācīta personāla.
* Darbinieku piekļuves ierobežošana personas datiem (saukta arī par "mazākās konfidencialitātes pielaides principu").
* Fiziskas drošības garantēšana telpās (piemēram, noteikumi personālam par dokumentu novietošanu slēgtā skapī darba dienas beigās, sensitīvās informācijas izdruku iznīcināšanu, kas vairs nav aktuālas, ievietojot tās konfidenciālā atkritumu tvertnē vai smalcinātājā).
* BYOD (“ņemiet līdzi savu mobilo ierīci”) principa ieviešana, ja ir atļauts izmantot personīgās ierīces darba vajadzībām.
* Stingra aizlieguma ieviešana attiecībā uz personīgā e-pasta izmantošanu darba vajadzībām.

**Vai ISO 27001 ieviešana atbilst ES VDAR prasībām?**

ISO 27001 ieviešana aptver lielāko daļu ES VDAR prasību; tomēr daži kontroles pasākumi jāpielāgo, lai personas dati tiktu iekļauti Informācijas drošības pārvaldības sistēmā.