BILDERLINGS PERSONAS DATU APSTRĀDES POLITIKA

Satura rādītājs

1. Par šo politiku

1.1. Starp Personas datu veidiem, ar ko **Bilderlings Group Companies**[1] ("**Bilderlings**", "**mēs**", "**mums**", "**mūsu**") var būt jārīkojas, ir informācija par esošajiem, bijušajiem un perspektīvajiem piegādātājiem, klientiem, izpildītājiem un jebkādiem citiem mūsu pakalpojumu lietotājiem (piemēram, mājaslapas lietotājiem) un citām personām, ar ko mēs komunicējam darbības nolūkos. Uz Personas datiem, kas var būt papīra formā, datorā vai citos datu nesējos, attiecas noteikti tiesiskie aizsardzības līdzekļi, tostarp tie, kas norādīti Vispārīgajā datu aizsardzības regulā, Regulā (ES) 2016/679 ("VDAR"), Latvijas Republikas Personas datu aizsardzības likumā, AK Datu aizsardzības likumā (2018) un citos noteikumos.

1.2. Šī politika un jebkādi citi tajā norādītie dokumenti kalpo par pamatu mūsu veicamajai Personas datu apstrādei, ko mēs iegūstam no Datu subjektiem, ko mums sniedz Datu subjekti vai kas ir iegūti no citiem avotiem. Datu lietotājiem ir pienākums ievērot šo Politiku, veicot Personas datu apstrādi mūsu vārdā. Jebkāds šīs politikas pārkāpums var izraisīt disciplināras sankcijas un ar likumu noteiktu atbildību. Šī politika pievēršas mūsu kā Datu pārziņa pienākumiem, un mums var būt atšķirīgi vai papildu pienākumi saistībā ar jebkādu apstrādi, ko mēs veicam kā Datu apstrādātājs.

1.3. Šī ir Politikas pašreizējā versija, un Atbildīgais par datu aizsardzību to pārskatīs vismaz vienu reizi gadā un periodiski atjauninās, lai atspoguļotu jebkādas izmaiņas normatīvajos aktos vai mūsu metodēs vai praksē. Šīs Politikas kārtējā versija būs pieejama mūsu mājaslapā Bilderlingspay.com vai pie Atbildīgā par datu aizsardzību.

1

Bilderlings Group ietilpst sabiedrības: AK reģistrēta sabiedrība Bilderlings Pay Limited, sabiedrības numurs: 09908958, juridiskā biroja adrese: 66 Prescot Street, Londona, Apvienotā Karaliste, E1 8NN, FCA atsauces numurs: 900637, un sabiedrība Bilderlings Pay SIA, kas reģistrēta Latvijas Republikā, reģ. Nr.: 40103869042, juridiskā adrese: Pils iela 8/10, Rīga, LV-1050.

2. Definīcijas

2.1. **Datu subjekti** nozīmē visas dzīvās, identificējamās personas, par kurām mūsu rīcībā ir Personas dati. Datu subjektam nav jābūt ES pavalstniekam vai pastāvīgajam iedzīvotājam. Visiem Datu subjektiem ir juridiskas tiesības attiecībā uz viņu personīgo informāciju.

2.2. **Personas dati** nozīmē datus attiecībā uz dzīvo personu, ko var tieši vai netieši identificēt pēc šiem datiem (vai pēc mūsu rīcībā esošiem datiem un citas informācijas). Personas dati var būt faktiski (piemēram, vārds, adrese vai dzimšanas datums) vai viedoklis vai apraksts par personu, tās rīcību un uzvedību.

2.3. **Datu pārziņi** ir personas vai organizācijas, kas nosaka nolūkus un veidus, kādos tiek apstrādāti jebkādi Personas dati. Pārziņiem ir pienākums noteikt praksi un politiku atbilstoši VDAR. **Datu lietotāji** ir mūsu darbinieki, pārstāvji, partneri un izpildītāji, kuru darbs saistīts ar Personas datu apstrādi. Datu lietotājiem vienmēr ir jāaizsargā dati, ar kuriem viņi rīkojas saskaņā ar šo datu aizsardzības politiku un jebkādu uz viņiem attiecināmu datu aizsardzības politiku.

2.4. **Datu apstrādātāju** skaitā ir jebkura persona vai organizācija, kas apstrādā Personas datus mūsu vārdā un pēc mūsu norādījumiem. No šīs definīcijas ir izslēgti Datu pārziņu darbinieki, bet tajā var būt iekļauti piegādātāji, kuri rīkojas ar Personas datiem mūsu vārdā.

2.5. **Mājaslapa** nozīmē mūsu mājaslapu: https://www.bilderlingspay.com/ .

2.6. **Apstrāde** ir jebkāda darbība vai darbību kopums, kas tiek veiktas ar Personas datiem vai Personas datu kopumiem, neatkarīgi no tā, vai tas notiek automatizētā veidā. Tajā skaitā ir datu iegūšana, ierakstīšana, turēšana vai jebkādu operāciju vai operāciju kopuma veikšanu ar datiem, tai skaitā to organizēšana, grozīšana, izgūšana, izmantošana, atklāšana, izdzēšana vai iznīcināšana. Apstrādē ietilpst arī Personas datu nodošana trešām personām.

2.7. **Profilēšana** nozīmē jebkāda veida automatizētu Personas datu apstrādi, kas sastāv no Personas datu izmantošanas, lai izvērtētu ar fizisko personu saistītus, konkrētus personības aspektus, it sevišķi, lai analizētu vai prognozētu tādus aspektus, kas attiecas uz šīs fiziskās personas veikumu darbā, ekonomisko situāciju, veselību, personīgajām izvēlēm, interesēm, uzticamību, uzvedību, atrašanās vietām vai pārvietošanos.

2.8. **Personas datu apstrādes politika** ir mūsu politikas jaunākā versija, kas pieejama Mājaslapā, attiecībā uz Personas datu iegūšanu, glabāšanu un izmantošanu (ar jebkurā laikā izdarītiem grozījumiem).

2.9. **Pseidonimizācija** nozīmē Personas datu apstrādi tādā veidā, lai Personas datus vairs nebūtu iespējams attiecināt uz konkrētu Datu subjektu, neizmantojot papildu informāciju, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tiek veikti tehniskie un organizatoriskie pasākumi, lai nodrošinātu to, ka Personas dati netiek attiecināti uz identificētu vai identificējamu fizisko personu. Jāņem vērā, ka pseidonimizēti dati joprojām ir Personas dati.

2.10. **Sensitīvi personas dati** attiecas uz informāciju par personas rasi vai etnisko izcelsmi, politiskajiem uzskatiem, reliģisko vai filozofisko pārliecību, piederību arodbiedrībai, fizisko vai garīgo veselību vai seksuālo dzīvi vai par jebkādu noziegumu, ko ir izdarījusi, vai tiek apgalvots, ka izdarījusi šāda persona, un šādas tiesvedības vai jebkuras tiesas pieņemta sprieduma kārtošana. VDAR kā Sensitīvi personas dati ir iekļauti biometriskie un ģenētiskie dati. Sensitīvus personas datus var apstrādāt tikai ar stingriem nosacījumiem, tai skaitā ar nosacījumu, ka nepieciešama attiecīgās personas īpaša atļauja, ja piemērojamais likums nenosaka citādi

2.11. **Pakalpojumi** nozīmē: (i) piekļuvi attiecīgajiem Bilderlings risinājumiem, izmantojot Klientu piereģistrēšanās saiti Bilderlings mājaslapā vai citu norādītu mājaslapu vai IP adresi; un/vai (ii) tiešsaistes vai ārsaistes papildproduktus un pakalpojumus, ko Bilderlings sniedz vai ir licencēta sniegt Klientam.

2.12. Reģistrs – Bilderlings Personas Datu apstrādes reģistrs, saskaņā ar VDAR 30.p. nosacījumiem.

3. Atbildība

3.1. VDAR atbildības princips noteic, ka organizācijām jāspēj demonstrēt datu aizsardzības prasību ievērošanu. Mums jānodrošina, lai datu aizsardzības ievērošana ir integrēta katrā jaunā tehnoloģiju plānošanā vai jaunās Apstrādes darbībās.

3.2. Atbildīgajam par datu aizsardzību (turpmāk – "ADA") ir pienākums nodrošināt VDAR un šīs Politikas ievērošanu. Bilderlings ir norīkojusi ADA, kura e-pasta adrese ir: DPO@bilderlings.eu.

Visi jautājumi par šīs politikas darbību vai jebkādas bažas par šīs politikas neievērošanu pirmām kārtām jāadresē Atbildīgajam par datu aizsardzību.

3.3. ADA ir neatkarīga amatpersona, kas iecelta šādu uzdevumu pildīšanai Bilderlings vārdā:

- Informēt un konsultēt mūsu Datu apstrādātājus, kuri veic mūsu Apstrādes darbības, par viņu pienākumiem, ko nosaka VDAR vai konkrētās jurisdikcijas datu aizsardzības noteikumi.
- Uzraudzīt, kā mēs ievērojam VDAR vai attiecīgos datu aizsardzības normatīvos aktus, kas attiecināmi uz mums, un uzraudzīt, kā mēs ievērojam savu politiku vai Datu apstrādātāju politiku.
- Pēc pieprasījuma sniegt padomu attiecībā uz datu aizsardzības ietekmes novērtējumu un uzraudzīt tā izpildi.
- Sadarboties ar uzraudzības iestādi un darboties kā uzraudzības iestādes kontaktpersonai ar Apstrādi saistītos jautājumos.

3.4. Datu subjekti var sazināties ar ADA visos jautājumos, kas attiecas uz viņu Personas datu apstrādi, un attiecībā uz savām VDAR noteiktajām tiesībām.

3.5. Visiem Bilderlings darbiniekiem ir pienākums ievērot VDAR un iziet atbilstošu apmācību, lai nodrošinātu šīs politikas ievērošanu. Lai nodrošinātu ADA nepieciešamo atbalstu pienākumu pildīšanā, šis amats ir pakļauts tieši Bilderlings atbildīgajai vadībai.

4. Datu aizsardzības principi

Visai Personas datu apstrādei jāatbilst labas prakses principiem. Tie nosaka, ka Personas datiem jābūt:

- Apstrādātiem godīgā, likumīgā un caurskatāmā veidā attiecībā pret personām.
- Iegūtiem konkrētos, īpašos un likumīgos nolūkos, neveicot turpmāku apstrādi ar šiem nolūkiem nesavienojamā veidā.
- Adekvātiem, būtiskiem un jāaprobežojas ar to, kas ir nepieciešams saistībā ar to apstrādes nolūku.
- Precīziem un atjauninātiem pēc nepieciešamības. Ja Personas dati ir neprecīzi to apstrādes nolūkā, jāveic visi pamatotie pasākumi, lai tos izdzēstu vai izlabotu bez kavēšanās.
- Turētiem tikai tik ilgi, cik tas nepieciešams Personas datu apstrādes nolūkā.
- Apstrādātiem atbilstoši Datu subjektu tiesībām.

- Apstrādātiem tādā veidā, kas nodrošina Datu subjekta atbilstošu drošību, tai skaitā aizsardzību pret nesankcionētu Apstrādi un nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu.
- Pasargātiem no nodošanas personām vai organizācijām valstīs, kurās nav nodrošināta adekvāta aizsardzība ar atbilstošu aizsardzības līdzekļu palīdzību.

5. Godīga un likumīga apstrāde

5.1. VDAR ir paredzēta nevis Personas datu apstrādes novēršanai, bet gan nodrošināšanai, lai tā tiek veikta godīgā, caurskatāmā veidā un bez negatīvas ietekmes uz Datu subjekta tiesībām. Konkrētajiem nolūkiem, kādos tiek apstrādāti Personas dati, jābūt īpaši un leģitīmi paziņotiem Datu subjektiem, un tiem jābūt noteiktiem Personas datu iegūšanas laikā.

5.2. Lai Personas datu apstrāde būtu likumīga, tā jāveic saskaņā ar VDAR noteiktajiem tiesiskajiem pamatiem. To skaitā, ir priekšnoteikums par Datu subjekta piekrišanuapstrādei un to,kaapstrāde nepieciešama līguma izpildei ar Datu subjektu, Datu pārzinim saistoša juridiska pienākuma izpildei vai Datu pārziņa vai tās puses, kurai dati tiek atklāti, leģitīmās interesēs. Sensitīvu personas datu apstrādes gadījumā jāievēro papildu nosacījumi. Apstrādājot Personas datus kā Datu pārzinis savas darbības ietvaros, mēs nodrošināsim šo prasību izpildi.

6. Apstrāde ierobežotos nolūkos

6.1. Savas darbības ietvaros mēs varam iegūt un apstrādāt Personas datus. To skaitā var būt dati, ko mēs saņemam tieši no Datu subjekta (piemēram, aizpildot formas, sarakstoties ar mums pa pastu, pa tālruni, e-pastu vai citādi), un dati, ko mēs saņemam no citiem avotiem (tai skaitā, piemēram, no darījumu partneriem, apakšuzņēmējiem tehniskos, maksājumu un piegādes pakalpojumos, kredītu atsauksmju sniedzējiem un citiem).

Mēs veiksim Personas datu apstrādi tikai konkrētos Personas datu apstrādes politikā noteiktos nolūkos vai jebkādos citos VDAR konkrēti atļautos nolūkos. Mēs paziņosim šos nolūkus Datu subjektam pirms datu iegūšanas. Mēs pastāvīgi pārskatīsim savus paziņojumus, lai pārliecinātos, vai tie precīzi atspoguļo mūsu apstrādes darbības, un, veicot datu apstrādi jaunā nolūkā, kas nav norādīts sākotnējā paziņojumā, mēs sniegsim jaunu paziņojumu, kurā šis nolūks būs iekļauts.

7. Datu subjektu kategorijas

7.1. Bilderlings iegūst un apstrādā dažādu informāciju par jums. Tai skaitā sekojošu informāciju:

- jūsu vārds, uzvārds, adrese (deklarētā/fakstiskā), personas kods un/vai dzimšanas datums, dzimums;
- kontaktinformācija, tai skaitā e-pasta adrese un tālruņa numurs;
- personas apliecinošā dokumenta kopija, numurs, izdošanas/derīguma datums, izdevējiestāde;
- informācija par jūsu valstisko piederību (t.sk. info par komunālmaksājumiem), bankas kontu, darba vietu;
- vai jebkādi citi personas dati un informācija, ko Bilderlings apstrādā saskaņā likumu, pārējiem vietējiem normatīvajiem aktiem vai starptautiskiem likumiem;

7.2. Bilderlings iegūst šo informāciju dažādos veidos. Piemēram, dati tiek iegūti no pieteikumu formām, CV vai kopsavilkumiem; tie tiek iegūti no jūsu pases vai ID kartes, no veidlapām, ko jūs aizpildāt darba uzsākšanas vai darba laikā (piemēram, atvieglojumu noteikšanas veidi), no korespondences ar jums vai no intervijām, tikšanās vai citiem novērtējumiem.

7.3. Dažos gadījumos Bilderlings var iegūt personas datus par jums no trešām personām, piemēram, iepriekšējo darba devēju atsauksmes, informāciju no nodarbinātības pamata informācijas pārbaudes veicējiem, informāciju no kredītu atsauksmju sniedzējiem un informāciju no sodāmības pārbaudēm, kas atļautas ar likumu, un citu pamatotu informāciju no citām institūcijām

8. Adekvāta, būtiska un samērīga apstrāde

8.1. Ja mēs iegūstam Personas datus tieši no Datu subjektiem, tā tiek:

- izmantota tikai tādā nolūkā vai nolūkos, kas ir noteikti mūsu Personas datu apstrādes politikā vai atļauti saskaņā ar VDAR;
- apstrādāta tikai tādā veidā, kāds ir noteikts mūsu Personas datu apstrādes politikā vai atļauts saskaņā ar VDAR; un
- atklāta tikai tādām trešām personām, kas noteiktas mūsu Personas datu apstrādes politikā vai atļautas saskaņā ar VDAR.

8.2. Saņemot Personas datus par Datu subjektu no citiem avotiem, mēs iespējami drīz pēc tam sniedzam šo informāciju Datu subjektam.

8.3. Bilderlings ir jāapstrādā dati, lai noslēgtu klienta līgumu ar jums un pildītu jūsu klienta līgumā noteiktos pienākumus.

8.4. Dažos gadījumos Bilderlings jāveic datu apstrāde, lai nodrošinātu savu juridisko pienākumu izpildi. Piemēram, jāpiemēro noziedzīgi iegūtu līdzekļu legalizācijas novēršanas normatīvie akti.

8.5. Citos gadījumos Bilderlings ir leģitīmas intereses apstrādāt personas datus pirms darba vai līguma attiecību sākumā, to laikā un pēc to beigām.

9. Precīzi dati

Mēs nodrošināsim, lai visi mūsu rīcībā esošie Personas dati ir precīzi un aktuāli. Mēs pārbaudām visu Personas datu pareizību to iegūšanas brīdī un ar regulāriem intervāliem pēc tam. Mēs veicam visus pamatotos pasākumus neprecīzu vai novecojušu datu iznīcināšanai vai izmainīšanai.

10. Neturēt ilgāk, nekā tas nepieciešams noteiktajā nolūkā

10.1. Mēs neturēsim Personas datus ilgāk, nekā tas nepieciešams Pakalpojumu izmantošanai vai sniegšanai un/vai tādā nolūkā vai nolūkos, kādos tie iegūti. ADA periodiski pārbaudīs turētos datus pēc to iegūšanas grafika.

10.2. Personas dati tiks turēti tik ilgi, kamēr tas nepieciešams Pakalpojumu sniegšanai un mūsu Personas datu apstrādes politikā norādīto nolūku izpildei. Piemēram, mēs turēsim Datu subjektu Personas datus tik ilgi, kamēr viņi turpina izmantot Pakalpojumus vai dot ieguldījumu to sniegšanā, un pamatotu laiku pēc tam, kā norādīts Reģistrā, izņemot gadījumu, ja likums nosaka vai atļauj ilgāku turēšanas periodu.

10.3. Līguma termiņa laikā Klienti var eksportēt ar Pakalpojumiem apstrādāto Klientu datu kopiju. 30 dienu laikā no attiecīgā Pakalpojuma izbeigšanas Klienti var: 1) pieprasīt Pakalpojumu sniegšanai iesniegto Klientu datu atdošanu; vai 2) piekļūt savam kontam, lai eksportētu vai lejupielādētu Pakalpojumu sniegšanai iesniegtos Klientu datus.

10.4. Pēc Pakalpojuma izbeigšanas, kad pagājis 30 dienu termiņš Klienta datu atdošanai, Pakalpojumu sniegšanai iesniegtie Klienta dati tiek turēti neaktīvā statusā līdz 90 dienām, un pēc tam tie tiek izdzēsti vai droši pārrakstīti, ja likums nenosaka citādi

11. Datu aizsardzības ietekmes novērtējums

11.1. Ja tiek ieviestas jaunas Apstrādes darbības vai mēs attīstām jaunas tehnoloģijas savā darbībā, jāveic operāciju izmaiņu ietekmes uz šādu Personas datu aizsardzību novērtējums, lai pievērstos visām Apstrādes operācijām, kas rada augstu risku Datu subjektu tiesībām un brīvībām vai VDAR neievērošanas risku.

11.2. Šāds novērtējums tiks veikts, konsultējoties ar Atbildīgo par datu aizsardzību.

12. Apstrādes darbību dokumentācija

Mēs dokumentēsim mūsu veiktās Apstrādes darbības (Reģistrā). Dokumentācija saturēs šādu informāciju:

- Datu pārziņa vārds un kontaktinformācija.
- Apstrādes nolūks.
- Datu subjektu kategoriju un Personas datu kategoriju apraksts.
- Saņēmēju kategorijas, kurām ir atklāti vai tiks atklāti Personas dati, tai skaitā saņēmēji trešās valstīs vai starptautiskas organizācijas, un dokumentācija par piemērotiem aizsardzības līdzekļiem sakarā ar šādu atklāšanu.
- Dažādu datu kategoriju dzēšanas termiņu.

13. Apstrāde atbilstoši Datu subjekta tiesībām

13.1. Mēs veiksim visu Personas datu apstrādi atbilstoši Datu subjektu tiesībām, it sevišķi noteiktos apstākļos atbilstoši viņu tiesībām:

- Pieprasīt piekļuvi jebkuriem datiem, kas ir Datu pārziņa rīcībā par viņiem, parasti izmantojamā un mašīnlasāmā formātā.
- Nodot savus datus citam Datu pārzinim (bez maksas), ja šādu Personas datu apstrāde notiek uz piekrišanas vai līguma izpildes pamata, izņemot gadījumu, ja tas var ietekmēt citu Datu subjektu vai citu personu tiesības un brīvības, tostarp komercnoslēpumus vai intelektuālo īpašumu.
- Novērst savu datu apstrādi vai noteiktos apstākļos atsaukt savu piekrišanu jebkurā laikā.
- Pieprasīt neprecīzu datu izmainīšanu.
- Dzēst savus personas datus, ja tie vairs nav nepieciešami sākotnējā nolūkā, vai tad, ja Datu subjekts ir atsaucis savu piekrišanu, un nepastāv nekādi citi tiesiski pamati apstrādes veikšanai.
- Iebilst pret savu Personas datu apstrādi noteiktos apstākļos.

- Būt informētiem par to, ka viņu Personas dati ir pakļauti automatizētai lēmumu pieņemšanai, t.i., profilēšanai, tai skaitā par iesaistīto loģiku, kā arī par šādas apstrādes nozīmīgumu un paredzamajām sekām Datu subjektam, un iebilst pret šādu profilēšanu noteiktos apstākļos.

13.2. Ja mums jāizsniedz Personas datu kopija, tas notiek bez maksas, bet par jebkādām pieprasītām papildu kopijām var tikt aprēķināta pamatota maksa, pamatojoties uz administratīvajām izmaksām.

13.3. Ja mēs pārtraucam apstrādāt Personas datus vai izdzēšam Datu subjekta Personas datus, tas potenciāli nozīmē, ka konkrētais Datu subjekts nespēj izmantot dažus mūsu Pakalpojumus vai dot ieguldījumu to sniegšanā, un par to tiks attiecīgi paziņots.

13.4. Ja Datu subjekts pieprasa labot vai dzēst savus Personas datus (izņemot datus, ko prasa jebkādi juridiski pienākumi) vai ierobežot šādu Personas datu apstrādi, mums var būt jāpaziņo par šādu pieprasījumu noteiktām trešām personām, kurām ir atklāti šie Personas dati.

14. Datu drošība

14.1. Turpmāk politikā aprakstīts, kā Bilderlings rīkojas ar personas datiem organizācijas ietvaros, un svarīgākie datu privātumu principi, kas tiek ievēroti. Šī nodaļa ir koncentrēta uz Bilderlings kā datu pārziņa lomu, un tā nav Bilderlings datu apstrādes pielikuma sastāvdaļa.

14.2. Bilderlings ir ieviesusi kārtību, kādā tiek nodrošināta Klientu datu apstrāde tikai saskaņā ar Klienta norādījumiem, kā aprakstīts Pielikumā A (“Drošības kontrole”), visā Bilderlings un tās apstrādes apakšpakalpojumu sniedzēju apstrādes darbības ķēdē. Turklāt Pakalpojumu drošību vērtē iekšējais personāls un trešās puses, tai skaitā veic infrastruktūras neaizsargātības novērtējumus un lietotnes drošības novērtējumus.

14.3. Bilderlings izturas nopietni pret jūsu datu drošību. Bilderlings ir noteikta iekšējā politika un kontroles pasākumi, lai censtos garantēt to, ka jūsu dati netiek nozaudēti, nejauši iznīcināti, ļaunprātīgi izmantoti vai atklāti, un lai tiem varētu piekļūt tikai tās darbinieki savu pienākumu izpildei. Tomēr jāatceras, ka neviena metode pārsūtīšanai internetā un neviena elektroniskās glabāšanas metode nav 100% droša un uzticama, un mēs nevaram garantēt tās absolūtu drošību.

14.4. Ja Bilderlings nolīgst trešās personas apstrādāt personas datus tās vārdā, apstrāde notiek uz rakstisku norādījumu pamata par konfidencialitātes ievērošanu un pienākumu veikt atbilstošus tehniskos un uzņēmuma pasākumus, lai garantētu datu drošību.

14.5. Mēs uzturēsim datu drošību, aizsargājot Personas datu konfidencialitāti, integritāti un pieejamību, atbilstoši šādām definīcijām:

- **Konfidencialitāte** nozīmē to, ka datiem var piekļūt tikai personas, kas ir pilnvarotas tos izmantot.
- **Integritāte** nozīmē to, ka Personas datiem jābūt precīziem un piemērotiem tam nolūkam, kādā tie tiek apstrādāti.
- **Pieejamība** nozīmē to, ka tikai pilnvaroti lietotāji spēj piekļūt datiem, ja tie nepieciešami autorizētos nolūkos. Tādēļ Personas dati jāglabā apstiprinātās datu krātuvēs.

14.6. Drošības procedūru skaitā ir:

- **Fiziskās drošības kontroles pasākumi.** Bilderlings objektos ir noteikti kontroles pasākumi (piemēram, signalizācija, apmeklētāju pavadīšanas kārtība un piekļuves kontroles žetoni) nesankcionētas piekļuves novēršanai.
- **Droši slēdzami galdi un skapji.** Galdi un skapji jātur aizslēgti, ja tie satur jebkāda veida konfidenciālu informāciju. (Personīgā informācija vienmēr uzskatāma par konfidenciālu.)
- **Utilizācijas metodes.** Dokumenti papīra formā tiek smalcināti, bet dokumenti digitālos datu nesējos tiek fiziski iznīcināti vai arī droši pārrakstīti, kad tie vairs nav nepieciešami.
- **Iekārtas.** Datu lietotājiem jānodrošina, lai konfidenciālā informācija individuālos monitoros nav redzama garāmgājējiem, un jāizrakstās no saviem datoriem vai jāslēdz sesija, ja datori tiek atstāti bez uzraudzības.
- **Incidentu pārvaldība.** Bilderlings uztur drošības incidentu pārvaldības politiku un kārtību. Bilderlings bez kavēšanās paziņo iesaistītajiem Datu subjektiem par katru gadījumu, kad Bilderlings vai tās pārstāvji nesankcionēti atklāj viņu personas datus, ja Bilderlings par to kļūst zināms, ar Datu aizsardzības likumiem un Noteikumiem noteiktajā apjomā.
- **Tehniskie aizsardzības līdzekļi.** Bilderlings nodrošina tādu tehnisku un organizatorisku pasākumu pieņemšanu, kas garantē datu drošību un minimizāciju, tai skaitā antivīrusu, ielaušanās atklāšanas un lietotāju autentifikācijas pakalpojumus, kā arī nepieciešamības gadā pseidonimizāciju un datu šifrēšanu.

15. Personas datu nodošana uz valsti ārpus EEZ

15.1. Mēs varam nodot jebkādus mūsu rīcībā esošus Personas datus uz valsti ārpus Eiropas Ekonomikas zonas (“EEZ”), ja pastāv viens no šādiem nosacījumiem:

- Valsts (vai organizācija), kam tiek nodoti Personas dati, nodrošina adekvātu aizsardzības līmeni Datu subjekta tiesībām un brīvībām (piemēram, uz adekvātuma lēmumu, apstiprinātu saistošu korporatīvo normu, standarta līgumu klauzulu pamata).

- Datu subjekts ir sniedzis savu piekrišanu.
- Nodošana ir nepieciešama kāda VDAR norādīta iemesla dēļ, tai skaitā starp mums un Datu subjektu noslēgta līguma izpildi, vai Datu subjekta vitālu interešu aizsardzībai.
- Nodošana ir juridiski nepieciešama uz svarīgu sabiedrības interešu pamata vai juridisku prasību nodibināšanai, īstenošanai vai aizstāvībai.
- Nodošanu ir apstiprinājusi attiecīgā datu aizsardzības iestāde, ja mēs esam pierādījuši adekvātus aizsardzības līdzekļus Datu subjektu privātuma, viņu pamattiesību un brīvību aizsardzībai un viņu tiesību izmantošanai.

15.2. Ņemot vērā iepriekšējā 15.1. punkta prasības, Personas datus, kas atrodas mūsu rīcībā, var apstrādāt arī personāls ārpus EEZ, kas strādā mums vai kādam mūsu piegādātājam. Šāds personāls var būt iesaistīts, starp citu, līgumu izpildē ar Datu subjektu, maksājumu datu apstrādē un atbalsta pakalpojumu sniegšanā.

16. Personīgas informācijas atklāšana un kopīgošana

16.1. Ņemot vērā 15. punktu, mēs varam kopīgot mūsu rīcībā esošus Personas datus ar jebkuru mūsu Grupas dalībnieku.

16.2. Mēs varam atklāt mūsu rīcībā esošos Personas datus arī trešām personām:

- Ja mēs pārdodam vai pērkam jebkādus uzņēmumus vai aktīvus, un tādā gadījumā mēs atklājam mūsu rīcībā esošos Personas datus šādu uzņēmumu vai aktīvu perspektīvajam pārdevējam vai pircējam pēc nepieciešamības.
- Ja trešā persona iegūst mūsu uzņēmumu vai pamatā visus mūsu aktīvus, un tādā gadījumā mūsu rīcībā esošie Personas dati ir nododamo aktīvu skaitā.
- Ja mums ir pienākums atklāt vai kopīgot Datu subjekta personas datus, lai izpildītu jebkādu juridisku pienākumu vai izpildītu vai piemērotu jebkādu līgumu ar Datu subjektu vai citus līgumus, vai aizsargātu mūsu tiesības un īpašumu vai mūsu klientu un citu personu drošību. Tai skaitā ir informācijas apmaiņa ar citām sabiedrībām un organizācijām aizsardzībai pret krāpniecību un kredītu risku samazināšanai.

16.3. Mēs varam kopīgot mūsu rīcībā esošos Personas datus arī ar izvēlētām trešām personām, tai skaitā, bet ne tikai, mūsu darījumu partneriem, pakalpojumu sniedzējiem un apakšuzņēmējiem jebkāda ar viņiem vai Datu subjektu noslēgta līguma izpildei, ja mēs sniedzam attiecīgu paziņojumu Datu subjektiem.

16.4. Personas datu atklāšana/kopīgošana ārpus mūsu organizācijas rada papildu riskus, un mums jānodrošina atbilstošo organizatorisko, tehnisko un līgumisko pasākumu veikšana pirms Personas datu nodošanas vai piekļuves nodrošināšanas.

17. Subjektu piekļuves pieprasījumi

17.1. Saskaņā ar VDAR datu subjektiem ir dažādas tiesības piekļūt Personas datiem, labot un dzēst tos un ierobežot to apstrādi. To skaitā ir tiesības:

- pēc pieprasījuma piekļūt saviem datiem un saņemt to kopiju;
- pieprasīt, lai Bilderlings izmaina nepareizus vai nepilnīgus datus;
- pieprasīt, lai Bilderlings izdzēš jūsu datus vai pārtrauc to apstrādi, piemēram, ja dati vairs nav nepieciešami apstrādes nolūkos;
- iebilst pret jūsu datu apstrādi, ja apstrādes tiesiskais pamats ir Bilderlings leģitīmās intereses; un
- prasīt, lai Bilderlings pārtrauc datu apstrādi uz laiku, ja dati ir neprecīzi, vai tad, ja pastāv strīds par to, vai jūsu intereses ir svarīgākas par Bilderlings veiktās apstrādes leģitīmajiem pamatiem.

17.2. Datu subjektiem jāiesniedz oficiāli pieprasījumi par informāciju, kas mūsu rīcībā ir par viņiem. Tiem jābūt rakstveidā. Darbiniekiem, kuri saņem rakstisku pieprasījumu, nekavējoties jāpārsūta tas Atbildīgajam par datu aizsardzību.

17.3. Mūsu darbinieki nodos pieprasījumu Atbildīgajam par datu aizsardzību palīdzības sniegšanai grūtās situācijās. Darbiniekus nedrīkst mudināt uz personīgas informācijas atklāšanu.

17.4. Visi Datu subjektu pieprasījumi jāizskata viena mēneša laikā no to saņemšanas, un Datu subjektiem nedrīkst aprēķināt maksu par šāda pieprasījuma iesniegšanu.

17.5. Mēs neaprēķinām maksu par Datu subjektu piekļuves pieprasījumu, izņemot gadījumu, ja mūsu saņemtie pieprasījumi ir pārmērīgi, atkārtojas vai ir acīmredzami nepamatoti, un tādā gadījumā mēs varam aprēķināt viņiem administratīvo maksu par šādu pieprasījumu apstrādi vai atteikties veikt darbības uz šādu pieprasījumu pamata.

18. Ziņošana par pārkāpumiem

18.1. Ja noticis Personas datu pārkāpums un pastāv iespēja, ka tas var radīt augstu risku Datu subjekta tiesībām un brīvībām, mēs bez liekas kavēšanās ziņosim par pārkāpumu Informācijas komisāra birojam, ja iespējams, ne vēlāk kā 72 stundu laikā pēc fakta uzzināšanas.

18.2. Ja noticis Personas datu pārkāpums un pastāv iespēja, ka tas var radīt augstu risku Datu subjekta tiesībām un brīvībām, mēs bez liekas kavēšanās ziņosim par pārkāpumu Datu subjektam. Paziņojumā Datu subjektam būs aprakstīts Personas datu pārkāpuma raksturs, kā arī ieteikumi, kas Datu subjektam jāņem vērā, lai mazinātu iespējamās negatīvās sekas. Šādi paziņojumi Datu subjektiem tiks sniegti iespējami drīzā laikā un ciešā sadarbībā ar uzraudzības iestādi, ievērojot šīs iestādes vai citu kompetento iestāžu, piemēram, tiesībsargājošo iestāžu norādījumus.

19. Dokumentu kontrole

APSTIPRINĀŠANA UN PIEDERĪBA

Izstrādāja	Amats	Datums	Vārds
Politikas autors	ADA	02.05.2018.	Sergejs Kravčenko
Apstiprināja	**Amats**	**Datums**	**Vārds**
Atbildīgais sponsors	Valdes loceklis	03.05.2018.	Andrejs Kuzins

PĀRSKATĪŠANAS VĒSTURE

Versija	Pārstrādāšanas datums	Pārskatīšanas datums	Apraksts
Sākotnējā			

Pielikums A. Datu apstrādātāja drošības kontroles pasākumi

1. Apstrādes raksturs un nolūks

1.1. Bilderlings apstrādā Personas datus, kas nepieciešami Bilderlings pakalpojumu sniegšanai, un atbilstoši Klienta papildu norādījumiem, izmantojot tos kā Datu pārziņa Pakalpojumus. Tai skaitā ir Personas datu automatizēta apstrāde, lai izvērtētu un analizētu atsevišķus ar Datu subjektu saistītus personīgos aspektus, un it sevišķi, lai analizētu vai prognozētu aspektus, kas attiecas uz Datu subjekta personīgajām izvēlēm, interesēm, uzvedību un atrašanās vietu.

2. Datu subjektu kategorijas

2.1. Klients var iesniegt Bilderlings dienestiem Personas datus tādā apjomā, kādu Klients nosaka un kontrolē pēc saviem ieskatiem, un to skaitā var būt, bet ne tikai, ar šādām datu subjektu kategorijām saistīti Personas dati:

- Klienta esošie un perspektīvie klienti, darījumu partneri un pārdevēji (fiziskās personas);
- Klienta esošo un perspektīvu klientu, darījumu partneru un pārdevēju darbinieki vai kontaktpersonas;
- Klienta darbinieki, pārstāvji, konsultanti, ārštata darbinieki (fiziskās personas);
- Klienta lietotāji, ko Klients ir pilnvarojis izmantot Pakalpojumus.

3. Personas datu veidi

3.1. Saistībā ar Pakalpojumu izmantošanu Klients var iesniegt vai atļaut iegūt Personas datus, kuru apjomu nosaka un kontrolē Klients pēc saviem ieskatiem, un to skaitā var būt, bet ne tikai, šādas Personas datu kategorijas:

- Vārds un uzvārds;
- Amata nosaukums;
- Ieņemamais amats;
- Darba devējs;
- Kontaktinformācija (uzņēmums, e-pasts, tālrunis, fiziskā darījumu adrese);
- Personas dokumenta dati;
- Uzvedības un profila dati;

- Personīgās izvēles;
- Savienojumu dati;
- Atrašanās vietas dati;
- Citi dati un informācija saskaņā ar likumu, pārējiem vietējiem normatīvajiem aktiem vai starptautiskiem noteikumiem.

4. Datu segregācija

4.1. Pakalpojumu vadība notiek arhitektūrā ar vairākiem nomniekiem, kas ir paredzēta Klienta datu glabāšanas un piekļuves tiem segregācijai un ierobežošanai, pamatojoties uz darījumu vajadzībām. Šī arhitektūra nodrošina efektīvu loģisko datu nodalīšanu par dažādiem Klientiem ar klientiem specifisku, unikālu ID palīdzību, un tā ļauj klientam un lietotājam izmantot piekļuves privilēģijas atkarībā no viņu lomas. Papildu datu segregāciju nodrošina nošķirta vide dažādām funkcijām, it sevišķi pārbaudīšanai un izgatavošanai.

5. Drošības kontroles pasākumi

5.1. Bilderlings ir ieviesusi kārtību, kas garantē to, ka Klienta dati tiek apstrādāti tikai atbilstoši Klienta norādījumiem visā Bilderlings un tās apakšuzņēmēju apstrādes darbību ķēdē. Turklāt iekšējais personāls un trešās personas veic Pakalpojumu drošības novērtējumu, tai skaitā infrastruktūras neaizsargātības novērtējumu un lietotnes drošības novērtējumu.

5.2. Bilderlings izmanto vairākus drošības kontroles pasākumus, kuru skaitā ir šādi:

- unikāli lietotāji identifikatori, kas ļauj Klientiem piešķirt saviem lietotājiem unikālus akreditācijas datus un piešķirt un pārvaldīt ar to saistītās atļaujas un tiesības;
- kontroles pasākumi, lai nodrošinātu sākotnējo paroļu pāriestatīšanu pirmajā lietošanas reizē;
- kontroles pasākumi, lai ierobežotu paroles atkārtotu izmantošanu;
- paroles garuma un sarežģītības prasības;
- Klientiem ir iespēja integrēt vienreizējas pierakstīšanās (*Single Sign-On*) tehnoloģijas, lai tieši kontrolētu autentifikāciju un akreditācijas datu sarežģītību, termiņa beigas, konta atslēgšanu, IP balto/melno sarakstu veidošanu;
- Klientiem ir iespēja pārvaldīt savu lietotņu lietotājus, noteikt lomas un piešķirt atļaujas un tiesības Pakalpojumu ieviešanas ietvaros;
- lietotāju paroles tiek glabātas vienvirziena iekonservēta savienojuma formātā un netiek pārsūtītas bez šifrēšanas;

- paroles datu servera seifs tiek šifrēts, izmantojot 256-bit AES šifrēšanu;
- tiek uzturēti lietotāju piekļuves pierakstīšanās ieraksti, kas satur datumu, laiku, lietotāja ID, izmantoto URL vai identitātes ID, veikto operāciju (piekļuve, radīšana, rediģēšana, dzēšana);
- ja notikusi aizdomīga vai neatbilstoša piekļuve Pakalpojumiem, Bilderlings var iesniegt Klientam reģistrācijas žurnāla ierakstu dokumentāciju, lai sniegtu palīdzību tiesu ekspertīzes analīzē. Šis pakalpojums tiks sniegts klientiem atkarībā no laika un materiāliem;
- lietotāju piekļuves reģistrācijas žurnāli tiks saglabāti drošā, centralizētā saimniekdatorā, lai novērstu viltošanu;
- lietotāju piekļuves reģistrācijas žurnāli tiek saglabāti ne mazāk kā 90 dienas;
- Bilderlings personāls neveic noteiktas paroles iestatīšanu lietotāju vajadzībām.

6. Iekļūšanas atklāšana

6.1. **Bilderlings** vai pilnvarota neatkarīga trešā persona veic Pakalpojumu uzraudzību, lai konstatētu nesankcionētu iekļūšanu, izmantojot iekļūšanas atklāšanas mehānismus saimniekdatorā.

7. Drošības kontroles žurnāli

7.1. Visas Pakalpojumu sniegšanā izmantotās Bilderlings sistēmas, tai skaitā ugunsmūri, maršrutētāji, tīkla slēdži un operētājsistēmas, reģistrē informāciju savās sistēmas reģistra ierīcēs vai centralizētā sistēmžurnāla serverī (tīkla sistēmās), lai atvieglotu drošības pārbaudes un analīzi.

8. Incidentu pārvaldība

8.1. Bilderlings uztur drošības incidentu pārvaldības politiku un kārtību. Bilderlings bez liekas kavēšanās paziņo iesaistītajiem Klientiem par jebkādu Bilderlings vai tās pārstāvju veiktu Klientu datu nesankcionētu atklāšanu, par ko Bilderlings kļūst zināms, Datu aizsardzības likumos un noteikumos noteiktajā apjomā.

9. Lietotāju autentifikācija

9.1. Piekļuve Pakalpojumiem prasa derīga lietotāja ID un paroles kombināciju (vai caur integrētu Vienreizējas pierakstīšanās (*Single Sign-On*) mehānismu), kas ir šifrēta ar TLS pārsūtīšanas laikā, kā arī iekārtas specifisko informāciju par identitātes apstiprināšanu, kas aprakstīta iepriekš sadaļā "Drošības kontroles pasākumi". Pēc sekmīgas autentifikācijas tiek ģenerēts nejauši

izvēlēts sesijas ID un saglabāts lietotāja pārlūkprogrammā, lai saglabātu un izsekotu sesijas statusu.

10. Fiziskā drošība

10.1. Ražošanas datu centriem, ko izmanto Pakalpojumu sniegšanai, ir piekļuves kontroles sistēmas. Šīs sistēmas ļauj tikai autorizētam personālam piekļūt drošajām zonām. Šīs iekārtas ir projektētas, lai izturētu negatīvus laika apstākļus un citus pamatoti prognozējamus dabas apstākļus; tie ir nodrošināti ar diennakts apsardzi, divpakāpju piekļuves pārbaudi, tai skaitā biometrisko pārbaudi, un piekļuvi pavadoņa kontrolē, un strāvas traucējumu gadījumā tos atbalsta arī objektā izvietoti rezerves ģeneratori.

11. Uzticamība un rezerves kopijas

11.1. Visi infrastruktūras komponenti ir konfigurēti augstā pieejamības režīmā vai dublētā veidā. Visi Pakalpojumu sniegšanai iesniegtie Klientu dati ir saglabāti infrastruktūrā, kas atbalsta augstu pieejamību, un tai regulāri tiek izveidotas rezerves kopijas. Šie rezerves kopijas dati tiek turēti vismaz vienu mēnesi. Rezerves kopijas tiek pārsūtītas un saglabātas šifrētā formā un turētas sekundāro datu centrā.

12. Avārijas atgūšana

12.1. Pakalpojumu ražošanas sistēmas ir aizsargātas ar avārijas atgūšanas plāniem, kas paredz būtisko datu un pakalpojumu rezerves kopēšanu. Pastāv visaptveroša atgūšanas procesu sistēma, lai visīsākā iespējamā laikā atjaunotu uzņēmumam būtisko sistēmu darbību. Atgūšanas procesi datubāzes drošībai, sistēmu administrācijai, tīklu konfigurācijai un datiem nosaka personāla rīcības plānu procesu pieejamības atjaunošanai.

13. Ļaunprogrammatūras

13.1. Pakalpojumiem ir izveidoti kontroles pasākumi ar mērķi novērst un atklāt ļaunprogrammatūru iekļūšanu attiecīgajās Pakalpojumu platformās.

14. Datu šifrēšana

14.1. Pakalpojumi izmanto vai dod iespēju Klientiem izmantot nozarē pieņemtus šifrēšanas produktus, lai aizsargātu Klientu datus un komunikācijas pārsūtīšanas laikā starp Klienta tīklu un Pakalpojumiem, tai skaitā vismaz 128-bit TLS sertifikātus un 2048-bit RSA publiskās atslēgas.

15. Klientu datu atdošana

15.1. Līguma darbības laikā Klienti var eksportēt Pakalpojumu apstrādātās Klientu datu kopijas. 30 dienu laikā pēc attiecīgā Pakalpojuma izbeigšanas Klienti var: 1) prasīt Pakalpojumiem iesniegto Klientu datu atdošanu; vai 2) piekļūt savam kontam, lai eksportētu vai lejupielādētu Pakalpojumiem iesniegtos Klientu datus.

16. Klientu datu izdzēšana

16.1. Pēc Pakalpojuma izbeigšanas, kad pagājis 30 dienu termiņš Klientu datu atdošanai, Pakalpojumiem iesniegtie Klientu dati tiek turēti neaktīvā statusā uz laiku līdz 90 dienām, un pēc tam tie tiek pārrakstīti vai arī izdzēsti, ja likumi, noteikumi vai citas mūsu saistības neliek mums rīkoties citādi.

17. Ziņošana par lietojumu un tendencēm

17.1. Bilderlings var izsekot un analizēt Pakalpojumu lietojumu drošības nolūkos, kā arī nolūkā palīdzēt Bilderlings uzlabot gan Pakalpojumus, gan lietotāju pieredzi Pakalpojumu izmantošanā. Piemēram, mēs varam izmantot šo informāciju, lai izprastu un analizētu tendences vai izsekotu, kādas mūsu iezīmes visbiežāk tiek izmantotas produktu funkcionalitātes uzlabošanai.

17.2. Var kopīgot anonīmus lietojuma datus ar Bilderlings pakalpojumu sniedzējiem, lai palīdzētu Bilderlings šādā izsekošanā, analīzes un uzlabojumu veikšanā. Turklāt Bilderlings var kopīgos šādus anonīmus datus kā kopumu parastā darbības gaitā; piemēram, mēs varam publiski kopīgot informāciju, lai parādītu mūsu Pakalpojumu vispārīgā lietojuma tendences.

18. Apstrādes apakšpakalpojumu sniedzēji

18.1. Bilderlings un tās saistītie uzņēmumi ir noslēguši rakstveida līgumus ar saviem apstrādes apakšpakalpojumu sniedzējiem, kas satur privātuma, datu aizsardzības un datu drošības pienākumus, lai nodrošinātu viņu apstrādes darbībām atbilstošu aizsardzības līmeni.

18.2. Izmanto šādu apstrādes apakšpakalpojumu sniedzēju pakalpojumus Bilderlings infrastruktūras ietvaros Klientu datu turēšanai un Pakalpojumu sniegšanai:

- **Karšu maksājumu nodrošināšanai** – SIA Worldline Latvia (reģ. Nr. 40003072814, Dzirnavu iela 37, LV-1010, Rīga)
- **Karšu maksājumu nodrošināšanai (kā saņēmējs)** – BlueOrangeBank JSC (Reģ. Nr. 40003551060, Smilšu iela 37, LV-1050, Rīga)
- **Datu glabāšanas un e-pasta pakalpojumiem MSO365** – Squalio LLC JSC (Reģ. Nr. 40003351675, Krišjāņa Valdemāra 21-19, LV-1010, Rīga)
- **Klientu resursu pārvaldībai** – SalesForce.com INC. (Reģ. Nr. The Landmark @ One Market street, San Francisco, CA 94105, ASV)
- **Apdrošināšanas priekšlikumu sagatavošanai** – AAS ERGO (Reģ. Nr. 40003131253, Skanstes iela 50, LV-1013, Rīga)
- **Maksājumu pakalpojumu nodrošināšanai** – SIA DEAC (Reģ. Nr. 40103255973, Maskavas iela 459, LV-1063, Rīga)

19. Eiropas specifiskie noteikumi – nodošana uz ārvalstīm

19.1. VDAR nosaka, ka Personas datus nedrīkst nodot uz valsti vai teritoriju ārpus Eiropas Ekonomikas zonas (t.i., ES dalībvalstis plus Islande, Lihtenšteina un Norvēģija, Apvienotā Karaliste – pēc 2019. gada 29. marta), izņemot gadījumu, ja šī valsts, teritorija vai organizācija nodrošina adekvātu aizsardzības līmeni Datu subjektu tiesībām un brīvībām saistībā ar Personas datu apstrādi.

19.2. Ņemot vērā 3.20. punktu, ja Klienta struktūra un Bilderlings struktūra atrodas EEZ, Bilderlings nedrīkst nodot Personas datus uz valsti ārpus EEZ bez Klienta iepriekšējas rakstveida piekrišanas, izņemot nodošanu un saņemšanu no: (i) jebkuras valsts, kas ir saņēmusi derīgu atbilstības lēmumu no Eiropas Komisijas; vai (ii) jebkuras organizācijas, kas nodrošina adekvātu aizsardzības līmeni atbilstoši spēkā esošajiem Datu aizsardzības likumiem un noteikumiem.