Informācijas drošības prasības
Versija C

1 Ievads drošības prasībās

Šī drošības prasību pielikuma mērķis ir noteikt minimālās Drošības prasības, kas piemērojamas Piegādātājam saistībā ar pakalpojumu sniegšanu vai produktu piegādēm (turpmāk visas sauktas - "**Piegādes**") Carlsberg grupas uzņēmumam. Carlsberg piešķir lielu nozīmi piegādāto produktu un pakalpojumu drošībai un uzticamībai. Tādēļ Piegādātājam ir pienākums veikt visus saprātīgi nepieciešamos pasākumus, lai aizsargātu Carlsberg datus un Aktīvus pret neatļautu piekļuvi, zādzību vai bojājumiem, kas varētu apdraudēt Carlsberg datu un Aktīvu konfidencialitāti, integritāti un pieejamību. Piegādātāja pienākums ir nodrošināt, ka atbilstība visām šajā pielikumā noteiktajām prasībām attiecas arī uz apakšuzņēmējiem, ar kuriem Piegādātājs noslēdz līgumus vai ar kuriem tas ir saistīts.

1.1 Piegādātāja atbilstība drošības prasībām

Piegādātājs ir atbildīgs par pilnīgu atbilstību šajā drošības pielikumā noteiktajām prasībām. Ja Piegādātājs konstatē jebkādu neatbilstību šeit noteiktajām prasībām, tas bez nepamatotas kavēšanās īsteno visus nepieciešamos un samērīgos koriģējošos pasākumus, lai atjaunotu atbilstību.

1.2 Piegādātāja pienākums paziņot par neatbilstībām

Piegādātājs nekavējoties informē Carlsberg par jebkādiem konfliktiem vai pretrunām starp prasībām, standartiem vai dokumentiem, kas minēti šajā drošības pielikumā. Carlsberg nosaka piemērojamo risinājumu, un Piegādātājs to ievēro.

1.3 Normatīvās prasības

Piegādātājs proaktīvi risina draudus, kuriem ir tieša ietekme uz Piegādēm un/vai Carlsberg datiem vai Aktīviem, un ievēro informācijas Drošības prasības, kā arī prasības attiecībā uz privātuma aizsardzību un Personas datu aizsardzību saskaņā ar Piemērojamiem likumiem, noteikumiem un kompetentu iestāžu lēmumiem. Jebkura konstatētā neatbilstība šādām prasībām tiek dokumentēta un novērsta.

2 Kontaktpunkts

Piegādātājs norīko vienu kontaktpersonu Carlsberg visos jautājumos, kas saistīti ar informācijas drošību un privātumu Piegāžu izpildes ietvaros. Šī persona kalpo kā galvenā kontaktpersona sadarbībai ar Carlsberg drošības jautājumos un ir pieejama, lai atbildētu uz jautājumiem, incidentiem un koordinācijas pieprasījumiem pēc nepieciešamības.

3 Prasības

3.1 Drošības pārvaldība un riska vadība

Piegādātājs izveido atbilstošu drošības pārvaldības sistēmu ar skaidri noteiktām lomām un atbildībām informācijas drošības jomā, uztur informācijas drošības politiku un atbilstošu dokumentāciju par Drošības kontroles pasākumiem. Pamatojoties uz regulāriem dokumentētiem riska novērtējumiem, Piegādātājs ievieš un uztur saprātīgus un samērīgus administratīvos, tehniskos un fiziskos Drošības kontroles

pasākumus, kas atbilst atzītai nozares praksei un ir piemēroti Pakalpojumiem un Carlsberg datu sensitivitātei.

3.2 Datu izmantošana un konfidencialitāte

Piegādātājs izmanto Carlsberg datus tikai pakalpojumu sniegšanai, nodrošina to konfidencialitāti un aizsargā pret neatļautu piekļuvi, izpaušanu, grozīšanu vai zudumu.

3.3 Piekļuves kontrole

Piegādātājs uztur identitātes un piekļuves pārvaldības procedūras, ierobežo piekļuvi Carlsberg datiem un (ja piemērojams) Carlsberg sistēmām tikai pilnvarotām personām, pamatojoties uz nepieciešamības zināt un minimālo tiesību principu, savlaicīgi noņem piekļuvi darbiniekiem, kas pamet uzņēmumu, un izmanto daudzfaktoru autentifikāciju jebkurai piekļuvei sistēmām, kurās tiek glabāti vai Apstrādāti Carlsberg dati, vai piekļuvei Carlsberg sistēmām.

3.4 Aktīvu pārvaldība

Piegādātājs uztur visu Aktīvu uzskaiti un nosaka atbildību par tiem Aktīviem, kas tiek izmantoti Piegāžu nodrošināšanai vai kas apstrādā Carlsberg datus vai pieslēdzas Carlsberg sistēmām. Piegādātājs nodrošina, ka Aktīvi ir droši konfigurēti un atjaunināti (tostarp savlaicīga drošības ielāpu uzstādīšana un aizsardzības pret ļaunatūru, ja attiecināms).

3.5 Datu apstrāde

Piegādātājs nodrošina drošu Carlsberg datu pārsūtīšanu un, ja Piegādātājs glabā pats vai citur Carlsberg datus, nodrošina to aizsardzību uzglabāšanas laikā. Pēc Carlsberg pieprasījuma vai līguma izbeigšanas Piegādātājs nekavējoties atgriež vai droši dzēš Carlsberg datus.

3.6 Trešo pušu riska pārvaldība

Piegādātājs nodrošina, ka jebkurš apakšuzņēmējs, kuram ir piekļuve Carlsberg datiem vai Carlsberg sistēmām, tiek izvērtēts no drošības riska viedokļa un ir rakstveidā uzņēmies drošības saistības, kas nav mazāk aizsargājošas kā šajā pielikumā noteiktās.

3.7 Incidentu pārvaldība

Piegādātājs uztur incidentu pārvaldības procedūras un bez nepamatotas kavēšanās (nekādā gadījumā ne vēlāk kā 24 stundu laikā) informē Carlsberg pēc tam, kad ir kļuvis zināms par jebkādu faktisku vai iespējamu Informācijas drošības incidentu, kas ietekmē Carlsberg datus vai Piegādes. Piegādātājs sadarbojas izmeklēšanas un seku novēršanas procesā un saglabā attiecīgos pierādījumus. Paziņojums tiek nosūtīts atbildīgajai kontaktpersonai un Carlsberg incidentu reaģēšanas komandai uz e-pasta adresi ThirdPartyIncidentNotification@carlsberg.com.

3.8 Darbības nepārtrauktība

Piegādātājs uztur saprātīgus un samērīgus darbības nepārtrauktības pasākumus, lai nodrošinātu Piegāžu nepārtrauktību un Carlsberg datu pieejamību. Piegādātājs periodiski testē savus darbības nepārtrauktības pasākumus.

3.9 Atbilstības apliecināšana

Pēc pieprasījuma (ne biežāk kā reizi gadā) Piegādātājs sniedz kopsavilkuma pierādījumus par drošības programmas efektivitāti (piemēram, rakstisku apliecinājumu vai pieejamas sertifikācijas).

3.10 Atbilstība

Piegādātājs nodrošina, ka tā darbinieki un apakšuzņēmēji, kas iesaistīti Piegāžu nodrošināšanā, ievēro Drošības prasības un Piemērojamos likumus (tostarp datu aizsardzības tiesību aktus), kas ir saistīti ar Piegādēm.

4 Vārdnīca

Terins	Definīcija
Piemērojamais likums	Jebkuri pārnacionāli, nacionāli valsts vai vietējās pašvaldības likumi, noteikumi u.c. normatīvie akti vai regulatīvās vadlīnijas (tostarp jebkuras prasības vai paziņojumi no jebkādas kompetentās uzraudzības iestādes), kā arī jebkādas obligātas uzraudzības iestāžu vadlīnijas, kas attiecas uz Carlsberg grupu vai tās uzņēmumiem.
Aktīvi	Jebkura ierīce, lietotne, sistēma, serveris, tīkla komponents vai pakalpojums, infrastruktūra, programmatūra.
Carlsberg dati	Jebkura informācija, dati, kas pieder vai kurus sniedzis Carlsberg
Piegādes	Konkrētie rezultāti, uzdevumi vai funkcijas, kurus Piegādātājam ir pienākums nodrošināt saskaņā ar Līgumu, tai skaitā gan ķermeniski produkti, gan pastāvīgi sniedzami pakalpojumi.
Informācijas drošības incidents	Veiksmīgi īstenots vai nenovēršams drauds, kas saistīts ar informācijas neatļautu piekļuvi, izmantošanu, izpaušanu, drošības pārkāpumu, grozīšanu, zādzību, nozaudēšanu, bojāšanu vai iznīcināšanu, kā arī ar iejaukšanos informācijas tehnoloģiju darbībā.
Personas dati	Jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu
Apstrādāšana	Jebkura darbība vai savstarpēji saistītu darbību kopums, kas tiek veikts ar informāciju neatkarīgi no tā, vai tas notiek automātiski vai citā veidā, piemēram, informācijas vākšana, reģistrēšana, nodrošināšana, organizēšana, glabāšana, pielāgošana vai grozīšana, piekļuve tai, tās iegūšana, izmantošana, izpaušana, dzēšana vai iznīcināšana.
Drošības kontrole	Jebkurš administratīvs, tehnisks, fizisks vai procesuāls pasākums, kura mērķis ir novērst, atturēt, atklāt, novērst sekas vai atjaunoties pēc draudiem, ievainojamībām, incidentiem vai neatbilstības, kas ietekmē informācijas konfidencialitāti, integritāti vai pieejamību. Termini “kontrole”, “aizsardzības pasākums” vai “riska pārvaldības pasākums” tiek lietoti kā sinonīmi.
Drošības prasības	Obligāto kontroļu, standartu un prakšu kopums, kas paredzēts sistēmu, datu un darbību aizsardzībai pret neatļautu piekļuvi, izpaušanu, izmaiņām vai iznīcināšanu.
Apakšuzņēmējs	Jebkura trešā persona, kuru Piegādātājs piesaista, lai izpildītu daļu no Pakalpojumiem vai Piegādēm. Apakšuzņēmējiem ir jāievēro visi piemērojamie šī Pielikuma noteikumi.