Bluerange Integritetspolicy KONSULT

Privacy Policy

Ver. #1.0

Denna integritetspolicy gäller för vår behandling
av våra kunders information i egenskap av
personuppgiftsbiträde enligt Dataskyddsförodningen

(EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679)

Bluerange Technologies AB
Österängsvägen 2, 554 63 Jönköping
Telefon: 036 – 34 59 00 Fax: 036 – 34 59 01
E-post: info@bluerange.se Webbplats: www.bluerange.se

Innehållsförteckning

Inledning 2
Viktiga GDPR-begrepp att känna till 3
Begreppsförklaringar 5
Dataskyddsombud 6
Ansvar 7
KUNDEN 7
LEVERANTÖREN 7
LEVERANTÖREN:s åtgärder, skyldigheter mm 8
Säkerhetsåtgärder 8
Incidenter 8
Överföring till tredje part 8
Underleverantörer 8
Särskild ersättning 9
Ansvar för skada 9
Avtalstid och upphörande 9
Tvist 9
Ändringar 9
LEVERANTÖREN:s säkerhetslösningar 10
Informationsskydd 10
Anlitad 3:e part 11
Zendesk 11

Inledning

Denna integritetspolicy beskriver hur Bluerange Sweden AB (556809-9492) med tillhörande bolag Bluerange Technologies AB (556533-2201) och Bluerange IT AB (556709-9394) hanterar våra kunders personuppgifter i enlighet med de delar av dataskyddsförordningens (EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679) krav som avser lagring och hantering av integritetskränkande information enligt GDPR (General Data Protection Regulation).

Ovan nämnda bolag kommer hädanefter gemensamt benämnas LEVERANTÖREN i detta dokument.

Detta dokument reglerar endast LEVERANTÖREN:s roll som *personuppgiftsbiträde* för de konsulttjänster vi utför åt våra KUNDER. Detta dokument reglerar INTE LEVERANTÖREN:s roll som *personuppgiftsbiträde* för LEVERANTÖREN:s drifttjänster. Denna information regleras i det separata dokumentet ”Bluerange Integritetspolicy DRIFT enligt Dataskyddsförordningen som personuppgiftsbiträde”.

Detta dokument reglerar heller INTE LEVERANTÖREN:s roll som *personuppgiftsansvarig* för den information LEVERANTÖREN lagrar om KUNDEN själv för att kunna leverera tjänster till KUNDEN. Denna information regleras i det separata dokumentet ”Bluerange Integritetspolicy enligt Dataskyddsförordningen som personuppgiftsansvarig”.

GDPR träder i kraft 2018-05-25.

Syftet med den nya lagstiftningen är dels att få till en harmonisering mellan EU:s medlemsstater. Dataskyddsdirektivet från 1995 utgjorde visserligen en gemensam grund inom unionen, men som direktiv var det upp till varje land att implementera regelverket och tolka det. Nu är det samma lagtext oavsett vilket EU-land man befinner sig i.

Samtidigt har det legat mycket fokus på ett ökat integritetsskydd. Medborgarnas rättigheter kommer att stärkas. Kraven på att företag och andra organisationer ska informera hur de hanterar uppgifter, vilka uppgifter och varför, de stärks. Det ska också gå att under vissa omständigheter säga nej till att personuppgifterna används.

I det ökade medborgarskyddet ingår också rätten att bli glömd. Alltså den chans en person har att begära att få uppgifter från exempelvis sökmotorer eller kundregister bortplockade. För det krävs att sökresultatet är oriktigt, irrelevant, eller överflödigt.

Detta dokument beskriver såväl KUNDEN som LEVERANTÖREN:s åtagande och ansvar gällande de tjänster KUNDEN nyttjar för KUNDEN:s lösning.

Viktiga GDPR-begrepp att känna till

Ansvarsskyldighet: Dataskyddsförordningen ställer stora krav på dokumentation och att man ska kunna visa att man efterlever lagen.

Behandling: Allting man gör med personuppgifter, till exempel samlar in, lagrar, ändrar, använder eller observerar, är en personuppgiftsbehandling.

Berättigat intresse: En av de sex möjliga grunderna för laglig behandling av personuppgifter. Berättigat intresse ska inte misstas för att vara en sorts ”carte blanche” som ger organisationer möjlighet att fortsätta som tidigare med sin behandling av personuppgifter. En så kallad intresseavvägning måste alltid göras om den här rättsliga grunden ska användas.

Dataskydd som standard: Det finns tekniska och organisatoriska krav på att organisationer säkerställer säker hantering av personuppgifter. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet.

Dataskyddsombud (DPO): Ny befattning med fler formella krav än personuppgiftslagens personuppgiftsombud, förkortas DPO efter engelskans Data Protection Officer. Många, men inte alla, verksamheter är skyldiga att utse dataskyddsombud och anmäla detta till Datainspektionen innan 25 maj 2018.

Incident: Om personuppgifter till exempel kommit på villovägar ska detta anmälas till Datainspektionen inom 72 timmar från det att man fick kännedom om incidenten. Ett gott samarbete med Datainspektionen är viktigt inte minst för att reducera de potentiellt väldigt höga böter som kan utfärdas.

Information: GDPR ställer stora krav på information till den registrerade, bland annat ska information vara lättbegriplig och GDPR definierar i många fall vilken information som måste lämnas i olika situationer.

Laglig grund: Dataskyddsförordningens artikel 6 listar olika lagliga grunder, varav en måste vara uppfylld för att personuppgiftsbehandling ska få göras.

Personuppgift: I princip vad som helst som direkt eller indirekt kan användas för att identifiera en fysisk person.

Personuppgiftsansvarig: Den juridiska person som ansvarar för personuppgifter.

Personuppgiftsbiträde: Underleverantör som den personuppgiftsansvarige använder för att hantera personuppgifter.

Personuppgiftsbiträdesavtal: Ett obligatoriskt avtal mellan den personuppgiftsansvarige och biträdet som reglerar vad personuppgiftsbiträdet ska, och får, göra med personuppgifterna som behandlas för den personuppgiftsansvariges räkning.

Pseudonymisering: En dataskyddsåtgärd som innebär att personuppgifter avidentifieras i den databas de normalt används, men att det finns en nyckel tillgänglig på annat håll. Ska inte förväxlas med kryptering eller anonymisering.

Samtycke: En av de sex möjliga grunderna för laglig behandling av personuppgifter. Samtyckesbegreppet utökas (kompliceras kan man kanske också säga) i förhållande till samtyckesbegreppet i personuppgiftslagen. Den som idag har inhämtat samtycke i enlighet med personuppgiftslagen har inte nödvändigtvis längre ett giltigt inhämtat samtycke när GDPR börjar tillämpas.

Uppgiftsminimering: En central princip i GDPR som handlar om att man inte får samla in fler personuppgifter än vad som är nödvändigt för ändamålet, och inte lagra uppgifter längre än nödvändigt.

Ändamål: Behandling av personuppgifter får endast ske med definierat ändamål, och detta får i princip inte ändras eller utökas i efterhand.

Överföring: GDPR reglerar hur överföring av personuppgifter får ske, i synnerhet om uppgifter lämnas ut till någon, exempelvis ett personuppgiftsbiträde, i ett så kallat tredje land – det vill säga utanför EU. Om Storbritannien inte får till något avtal med EU gällande dataskydd kommer även de att räknas som tredje land efter Brexit.

Begreppsförklaringar

Detta avsnitt beskriver de begrepp som används vidare i detta dokument.

LEVERANTÖREN
Bluerange Sweden AB
Org.nr: 556809-9492

Bluerange Technologies AB
Org.nr: 556533-2201

Bluerange IT AB
Org.nr: 556709-9394

KUNDEN
En juridisk person som nyttjar en eller flera av LEVERANTÖREN:s tjänster.

KUNDEN:s lösning
Med KUNDEN:s lösning avses såväl fysiskt skalskydd och infrastruktur som system och logiskt informationsskydd, i vilket KUNDENS information lagras och behandlas, och som LEVERANTÖREN har möjlig tillgång till.

Dataskyddsombud

Kontaktuppgifter till LEVERANTÖRENS dataskyddsombud
Nichlas Melin
Bluerange Sweden AB
Österängsvägen 2
554 63 JÖNKÖPING
Tel: +46 36 34 59 00
E-post: dataskydd@bluerange.se

Ansvar

Detta kapitel reglerar respektive parts ansvar för KUNDEN:s lösning.

KUNDEN

KUNDEN är skyldig att efterleva personuppgiftslagen samt, vid dess ikraftträdande, Dataskyddsförordningen, avseende personuppgiftsbehandling och anlitande av biträde.

LEVERANTÖREN är behjälplig i detta arbete genom att tillhandahålla rekommendationer och i förekommande fall konfigurationer av en säker IT-infrastruktur med reglerarad åtkomst, eller annan tjänst utförd av LEVERANTÖREN.

Om KUNDEN väljer att avstå från de åtgärder och tjänster som LEVERANTÖREN rekommenderar, eller om ytterligare åtgärder utanför LEVERANTÖREN:s kontroll behöver appliceras i KUNDEN:s lösning för att KUNDEN:s lösning skall uppfylla kraven enligt Dataskyddsförordningen, är KUNDEN självt ansvarig för att dessa appliceras på lösningen så att den i helhet uppfyller kraven enligt Dataskyddsförordningen.

LEVERANTÖREN

LEVERANTÖREN ansvarar för att den infrastruktur, de tjänster och åtgärder som tillhandahålls av LEVERANTÖREN är utformade och underhålls på ett sådant sätt att de i sig, vid var tid, uppfyller de tekniska kraven avseende skydd, lagring och behandling av känslig information enligt Dataskyddsförordningen och skyddar de registrerades rättigheter.

I de fall LEVERANTÖREN upptäcker brister eller fel i infrastrukturen, de tjänster och/eller åtgärder som tillhandahålls, eller om LEVERANTÖREN upptäcker att KUNDEN:s lösning blir utsatt för obehörigt intrång, är LEVERANTÖREN skyldig att utan oskäligt dröjsmål meddela KUNDEN detta.

LEVERANTÖREN har inget ansvar för KUNDEN:s lösning och dess innehåll eller hur den uppfyller kraven i Dataskyddsförordningen om inte annat avtalats.

Separat avtal upprättas, om så är applicerbart, som reglerar LEVERANTÖREN:s tillgång KUNDEN:s lösning.

LEVERANTÖREN ansvarar för att den egna verksamheten bedrivs på ett sätt som i övrigt säkerställer adekvat informationssäkerhet.

LEVERANTÖREN åtar sig att endast vidta personuppgiftsbehandling avseende avtalade personuppgifter i enlighet med eventuellt dokumenterade instruktioner från KUNDEN samt i överensstämmelse med detta dokument och eventuellt tillhörande huvudavtal.

För det fall LEVERANTÖREN saknar instruktioner som denne bedömmer är nödvändiga för att genomföra sina åtaganden skaLEVERANTÖREN, utan dröjsmål, meddela KUNDEN om detta och invänta vidare instruktioner.

LEVERANTÖREN:s åtgärder, skyldigheter mm

Detta avsnitt reglerar LEVERANTÖREN:s åtagande gällande säkerhetsarbete, åtgärder i samband med incidenter, överföring av data, anlitande av underleverantörer

Säkerhetsåtgärder

LEVERANTÖREN förbinder sig att föreslå, vidta och upprätthålla lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda KUNDEN:s lösning mot obehörig åtkomst.

LEVERANTÖREN ska tillse att anställda, konsulter och övriga som LEVERANTÖREN svarar för och som behandlar eller har åtkomst till KUNDEN:s lösning är bundna av ett ändamålsenligt sekretessåtagande samt är informerade om hur personuppgiftsbehandling får ske i enlighet med eventuella ytterligare instruktioner från KUNDEN.

LEVERANTÖREN förbinder sig att kontinuerligt genomföra kontroller och säkerhetsåtgärder av beskrivna tjänster för att säkerställa tillgänglighet och motståndskraft i systemen, samt att förmågan att återställa tillgänglighet och tillgång till KUNDEN:s lösning existerar i rimlig tid vid fysisk eller teknisk incident och förfarande för regelbunden testning, undersökning och utvärdering av effektiviteten hos säkerhetsåtgärderna.

Av säkerhetskäl och skydd mot potentiella hot om framtida intrång, attacker eller andra eventuella komprometterande händelser mot alla våra kunders information ges KUNDEN inte tillgång till insyn i vår organisation, dess processer eller vår infrastrukturs tekniska design och implementation, utan KUNDEN är hänvisad till den information som finns i våra tjänstebeskrivningar och i detta dokument.

Incidenter

LEVERANTÖREN ska vid konstaterad eller misstänkt säkerhetsincident, såsom obehörig åtkomst, förstörelse, ändring eller annan otillåten påverkan avseende KUNDEN:s lösning omedelbart undersöka incidenten, vidta lämpliga åtgärder i LEVERANTÖRENS infrastruktur och om möjligt åtgärda densamma för att förhindra upprepning samt informera KUNDEN genom att tillhandahålla Incidentrapport.

En incidentrapport ska åtminstone innehålla beskrivning av incidentens art, beskrivning av sannolika konsekvenser till följd av incidenten och en åtgärdsplan, om lämpligt inbegripet åtgärder för att mildra potentiella negativa effekter. Därtill ska incidentrapport innehålla kontaktuppgift(er) för erhållande av ytterligare information om incidenten.

Överföring till tredje part

LEVERANTÖREN får inte överföra eller lämna ut information om KUNDEN:s lösning till tredje man, utan att i förväg inhämta skriftligt godkännande av den KUNDEN, med undantag för när sådant utlämnande kan krävas enligt lag.

För de fall där tredje man begär ut information från LEVERANTÖREN som rör personuppgiftsbehandlingen ska LEVERANTÖREN utan onödigt dröjsmål vidarebefordra sådan framställan till KUNDEN.

LEVERANTÖREN har inte rätt att företräda KUNDEN eller agera för KUNDEN:s räkning gentemot tredje man.

Underleverantörer

För anlitande eller ersättande av underleverantör ej upptagna i detta dokument, för utförande av uppgift som innefattar KUNDEN:s lösning, ska LEVERANTÖREN först begära skriftligt godkännande för undertecknande

av behörig företrädare hos KUNDEN. Sådan begäran ska innehålla uppgift om underleverantörens bolagsnamn och kontaktuppgifter, tjänstetyp, säte och geografisk placering av infrastruktur relevant för behandlingen av personuppgifter, samt andra uppgifter om underleverantören som begärts av KUNDEN. KUNDEN har rätt att med bindande verkan motsätta sig anlitandet av viss underleverantör om rimligt fog därför finns.

Särskild ersättning

LEVERANTÖREN har inte rätt till särskild ersättning för fullgörandet av ansvar och skyldigheter enligt detta dokument för att upprätthålla de tjänster KUNDEN använder, annat än för de tjänster som framgår av respektive tjänsteavtal eller då det framgår av skriftlig överenskommelse.

Ansvar för skada

LEVERANTÖREN kan inte hållas ansvarig för händelser utanför LEVERANTÖREN:s kontroll så som blixtnedslag eller andra naturhändelser, brand, arbetskonflikt, myndighetsbestämmelse eller andra händelser över vilka LEVERANTÖREN inte rimligen kan råda.

LEVERANTÖREN kan heller inte hållas ansvarig för förluster kunden kan erhålla, varken ekonomiska eller fysiska, i samband med nyttjandet, av LEVERANTÖREN, tillhandahållna system och tjänster, varken under utvecklings/testfasen eller i kommersiell drift.

Avtalstid och upphörande

Detta dokument gäller för alla LEVERANTÖREN:s konsulttjänster som KUNDEN nyttjar och gäller under den tid respektive tjänst nyttjas om inget annat avtalats.

Tvist

Tvist angående tolkning eller tillämpning av detta avtal skall hänskjutas till skiljedom enligt Stockholms Handelskammares Skiljedomsinstituts regler för förenklat skiljeförfarande.

Ändringar

LEVERANTÖREN förbehåller sig rätten att förändra tjänsters utförande och innehåll. LEVERANTÖREN skall då utan onödigt dröjsmål meddela KUNDEN detta. KUNDEN har rätt att med bindande verkan motsätta sig en sådan ändring om den INTE uppfyller de tekniska kraven avseende lagring och behandling av känslig information enligt Dataskyddsförordningen och skyddar de registrerades rättigheter.

LEVERANTÖREN:s säkerhetslösningar

Detta avsnitt redogör för de åtgärder och lösningar LEVERANTÖREN använder för att skydda KUNDEN:s lösning från obehörigt tillträde.

Av säkerhetskäl och skydd mot potentiella hot om framtida intrång, attacker eller andra eventuella komprometterande händelser mot KUNDEN:s lösning ges här endast en principiell beskrivning utan tekniska detaljer över LEVERANTÖREN:S infrastruktur.

Informationsskydd

Detta avsnitt beskriver generellt hur vårt säkerhetsskydd avseende information principiellt är uppbyggt, med informationsskydd avses de tekniska lösningar som används för att förhindra intrång eller obehörig åtkomst av information i KUNDEN:s lösning.

LEVERANTÖREN lagrar alltid och endast ett administrativt konto med tillhörande lösenord för att kunna erbjuda kunden återställning av lösenord i de fall det behövs om inte annat avtalats.

KUNDEN erbjuds brandväggslösning för att reglera åtkomst till KUNDEN:s lösning.

KUNDEN erbjuds 2-faktorsautentisering för att reglera åtkomst till KUNDEN:s lösning

KUNDEN erbjuds möjlighet till krypterad internettrafik till och från KUNDEN:s lösning.

KUNDEN ansvarar för att KUNDEN:s lösning uppfyller de tekniska kraven avseende lagring och behandling av känslig information enligt Dataskyddsförordningen för att skydda de registrerades rättigheter.

LEVERANTÖREN ansvarar för att LEVERANTÖREN:s rekommendationer uppfyller de gängse normer och krav som ställs inom IT-branschen.

Anlitad 3:e part

KUNDEN ansvarar för att, av KUNDEN anlitad, 3:e part som behandlar eller har åtkomst till KUNDEN:s lösning är bundna av ett ändamålsenligt sekretessåtagande samt är informerade om hur personuppgiftsbehandling får ske i enlighet med Dataskyddsförordningen.

LEVERANTÖREN ska tillse att anställda, konsulter och övriga som LEVERANTÖREN svarar för och som behandlar eller har åtkomst till KUNDEN:s lösning är bundna av ett ändamålsenligt sekretessåtagande samt är informerade om hur personuppgiftsbehandling får ske i enlighet med eventuella ytterligare instruktioner från KUNDEN.

LEVERANTÖREN förbehåller sig rätten att byta underleverantör om LEVERANTÖREN bedömer att detta är nödvändigt för upprätthållandet av LEVERANTÖREN:s tjänster. LEVERANTÖREN skall då utan onödigt dröjsmål meddela KUNDEN detta. KUNDEN har rätt att med bindande verkan motsätta sig anlitandet av viss 3:e part om rimligt fog därför finns.

Zendesk

1019 Market St
San Francisco, CA 94103
888-670-4887
Tel: +1 (415) 418 7506

Zendesk tillhandahåller ett ärendehanteringsystem där LEVERANTÖREN hanterar LEVERANTÖREN:S ärenden för de tjänster LEVERANTÖREN tillhandahåller. I detta system kan vissa personuppgifter releterade till ärendet lagras och behandlas.

Mer information om Zendesk och deras åtagande kring GDPR hittar ni här:
https://www.zendesk.com/company/customers-partners/eu-data-protection/