BRP Systems och GDPR

Bakgrund

Dataskyddsförordningen, eller GDPR som den också kallas, innehåller regler om hur man får behandla personuppgifter. Förordningen börjar gälla den 25 maj 2018 och ersätter då personuppgiftslagen (PuL).

Vi på BRP Systems gör vårt yttersta för att erbjuda våra kunder verktyg som kan hjälpa personuppgiftsansvarig fullgöra skyldigheterna enligt förordningen. Just nu arbetar vi med att paketera vidareutveckling av basfunktionaliteten, valbara tillägg samt ett utbildningsprogram som hjälper er med grundläggande kunskap om GDPR och hjälp kring hur ni konfigurerar systemet.

Begrepp

Registrerad = Den person som registreras i systemet. I regel kunder eller anställda.
Systemet = Affärssystemet BRP Systems, exklusive integrationspunkter som hårdvara, kundanpassningar och integrationer med tredje part.
Systemleverantören = BRP Systems AB
Kunden = Juridisk person som köper tillgång till Systemet som tjänst av Systemleverantören
Personuppgift = Varje upplysning som avser en identifierad eller identifierbar fysisk person
Behandling = En åtgärd eller kombination av åtgärder beträffande personuppgifter
Pseudonymisering = Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används
Personuppgiftsansvarig = Juridisk person som registrerar personer. I detta fall bolaget som driver anläggningen.
Användare = En person som använder Systemet å Personuppgiftsansvarigs vägnar (i regel en anställd)

Om dokumentet

Detta dokument syftar till att internt och för Systemleverantörens kunder dokumentera:

1. Ansvarsfördelning mellan kunden och Systemleverantören
2. Systemleverantörens planerade utveckling av Systemet för att hjälpa våra kunder i samband med GDPR (åtgärderna i dokumentet är dock inte slutgiltiga och kan komma att ändras)
3. Potentiell framtida utveckling som kommer erbjudas som tillval av systemleverantören och inte kommer ingå i basfunktionaliteten av Systemet
4. Tips till våra kunder på konfigurationer och rutiner hänförliga till Systemet för att efterleva kraven i GDPR

Ansvar

Den som behandlar personuppgifter, t.ex. genom insamling, lagring eller på annat sätt, är antingen personuppgiftsansvarig eller personuppgiftsbiträde och GDPR uppställer olika krav och skyldigheter beroende på vilken kategori man tillhör.

- Personuppgiftsansvarig ansvarar för att tillse att behandling av personuppgifter som vidtas, av personuppgiftsansvarig självt eller på uppdrag av denne, sker i enlighet med GDPRs bestämmelser.
- Personuppgiftsbiträdet ansvarar för att ge tillräckliga garantier för att behandlingen uppfyller kraven i GDPR och säkerställa att den registrerades rättigheter skyddas.

Med avseende på behandling av personuppgifter inom ramen för Systemet är våra kunder generellt att anse som personuppgiftsansvariga och Systemleverantören är personuppgiftsbiträde.

Vi uppmanar våra kunder att tillsammans med en legal rådgivare överväga och bedöma hur GDPRs krav påverkar just er. Denna informationsbroschyr är endast avsedd att informera om hur Systemleverantörer arbetar i sina förberedelser inför GDPRs ikraftträdande och ska inte på något sätt ses som en komplett guide eller specifik rådgivning till nödvändiga åtgärder i samband med GDPR.

Utveckling av funktionalitet för GDPR

Vissa vidareutvecklingar av produkten blir en del av basfunktionaliteten. Andra blir tillgängliga som tillval. Prissättning för tillvalen meddelas vid en senare tidpunkt.

Resterande sidor i dokumentet beskriver Systemleverantörens planer för ny eller ändrad funktionalitet i Systemet. Åtgärderna är dock inte slutgiltiga och kan komma att ändras.

Informationen, den planerade utvecklingen och rutinerna är samlade under de områden av GDPR som de huvudsakligen berör.

Underrubriken “Rutiner” riktar sig till Personuppgiftsansvarig (systemadministratör eller övrig personal) med förslag i samband med konfiguration av den nya funktionaliteten samt vid daglig drift.

Avtal och samtycke (basfunktionalitet)

Information

Enklast ses alla köp av tjänster och andra produkter som ingångna avtal. För att leverera tjänsten behöver ni grundläggande personuppgifter för att kunna:

- Kommunicera med Registrerad (namn, adress, e-postadress och telefonnummer)
- Undvika dubletter vid registrering (personnummer)
- Hantera autogiro (personnummer)
- Avgöra ålder för exempelvis simskola, ungdomspriser (personnummer, födelsedatum)
- Erbjuda en säker träningsmiljö (inpasseringskontroll och besökslistor vid incidenter)
- Presentera träningsstatistik (besök och träningspass)
- Hantera frågor, reklamationer och återköp (bokningar och köp)

Ny funktionalitet

- Avtalsvillkor visas vid all registrering i internetbokning generation 2 (lanserad 2015).
- Be om samtycke för massutskick vid registrering i internetbokning.
- Vid manuell registrering ändras förvalt värde för massutskick till nej.
- Vid manuell registrering av person i gränssnitt för backoffice samt i kundrutiner, ställs en fråga till användaren om personen som registreras godkänt avtalsvillkoren innan personuppgifterna sparas. Användare och tidpunkt loggas.
- Möjlighet att vid massutskick via e-post från Systemet genom länk återkalla samtycket.
- Möjlighet att via internetbokning (generation 2) ändra samtycke till massutskick.

Rutiner

- Utforma ett tydligt avtal där ni berättar vilken information som lagras, varför och hur den används.
- Informera om att bild är frivilligt och att bilden kan komma att användas vid stickprovskontroller och på skärmar vid inpassering.
- Informera om integrationer och automatiska exporter som medför att kunduppgifter skickas till tredje part, samt varför dessa är nödvändiga för att ni ska kunna leverera tjänsten.
- Använder ni fortfarande internetbokning generation 1 (lanserad 2015) behöver ni extra noga se över om ni bedömer att ni kan uppfylla kraven i GDPR eftersom den produkten inte lägre utvecklas. Ett tips kan vara att inaktivera registrering i internetbokningen.

Begränsa lagring av personuppgifter (basfunktionalitet)

Information

För att pseudonymisering ska vara möjlig behöver personuppgifter så långt det är möjligt hållas till personobjektet så att en pseudonymisering blir fullständig.

Ny funktionalitet

- Vi övergår från att i loggar och historik använda namn och andra personuppgifter till att referera till personprofilen.

Rutiner

- Undvik att skriva in personuppgifter i meddelandefälten på bokningar och beställningar eller i andra fält utanför personkortet.

Begränsa tillgång till personuppgifter (basfunktionalitet)

Information

För att personuppgifter inte i onödan ska visas för användare som inte behöver dem införs nya rättigheter, möjligheter att begränsa resultat i sökningar och aktiv visning av uppgifter i kombination med loggning.

Ny funktionalitet

- Möjlighet att med systeminställning begränsa maximalt antal träffar för en sökning.
- Rättighet som ger vissa användare möjlighet till oändligt antal träffar i sökning.
- På personkortet är adress, e-postadress, telefonnummer, e-postadress, personnummer, födelsedag och kön dolda. Användaren kan aktivt välja att visa dem, och då loggas accessen med referens till användaren och tidpunkt.
- Rättighet som låter vissa användare se alla personuppgifter utan att access loggas.

Rutiner

- Konfigurera maximalt antal träffar vid personsökning
- Konfigurera personlistan i Systemet så att endast de kolumner som är absolut nödvändiga för att hitta den person man söker visas, kanske bara för och efternamn.
- Var återhållsam med rättigheterna som ger utökade rättigheter till sökning och access till personuppgifter.
- Var återhållsam med rättigheterna som ger tillgång till exporter av personlistor.
- Reglera i avtal vilka uppgifter API-integratörer och mottagare av automatiserade exporter får hantera.
- Se över avtal med kund om ni exporterar personuppgifter till tredje part, som integratörer eller externa e-postsystem.

Manuell pseudonymisering (basfunktionalitet)

Information

Pseudonymisering gör så att information som registrerats i Systemet inte längre kan tillskrivas en verklig person. När en registrerad person ska betraktas som ej aktiv och eventuellt pseudonymiseras beslutas av personuppgiftsansvarig.

Ny funktionalitet

- Rättighet som avgör vilka användare som får markera en person för pseudonymisering.
- Möjlighet att markera person för pseudonymisering (förutsatt att aktiva abonnemang, obetalda fakturor, kundkontoskulder eller framtida bokningar saknas).
- Rättighet som avgör vilka användare som får lista personer som markerats för pseudonymisering för att sedan slutföra pseudonymiseringen.
- Möjlighet att lista personer som markerats för pseudonymisering för att sedan gå vidare med slutgiltig pseudonymisering. Detta rensar bort alla personuppgifter men behåller personobjektet, bokningar, besök mm.
- Frikoppla avtal vid pseudonymisering (eftersom avtal innehåller personuppgifter).
- Frikoppla fakturor vid pseudonymisering (eftersom fakturor innehåller personuppgifter).
- Visa ej pseudonymiserade personobjekt i personlista.

Rutiner

- Ta beslut om vilka användare som får de nya rättigheterna
- Sätt upp en rutin för hur ni hanterar kunder som säger upp sitt abonnemang eller låter det löpa ut.
- Eftersom det inte är ovanligt att kunder återkommer och ångrar sin uppsägning eller tecknar ett nytt abonnemang kan ni om det passar verksamheten markera personer för pseudonymisering och sedan avvakta några veckor innan slutgiltig pseudonymisering.

Automatiserad pseudonymisering (tillval)

Information

En samling verktyg som med regler och automatisering underlättar pseudonymisering.

Ny funktionalitet

- Möjlighet att med inställningar ange när personer utifrån anställning, abonnemang, bokningar och besök ska betraktas som aktiva.
- Möjlighet att söka fram inaktiva personer och markera dem för pseudonymisering.
- Möjlighet att varje natt automatiskt markera inaktiva personer för pseudonymisering.
- Möjlighet att varje natt automatiskt slutgiltigt pseudonymisera personer som markerades för pseudonymisering för x dagar sedan.
- Möjlighet att markera valda personer som ska undantas från pseudonymisering, exempelvis kontaktpersoner på företag som saknar abonnemang eller bokningar.
- Möjlighet att med avancerat urval hitta personer undantagna vid pseudonymisering.
- Inställning för att även tömma fritextfält (som kan innehålla personuppgifter).
- Funktion som notifierar tredje part (integratörer) vid pseudonymisering.

Rutiner

- Ta beslut om tömning av fritextfält vid pseudonymisering
- Om inte slutgiltig pseudonymisering ska ske automatiskt, skapa en rutin för vem som gör det manuella steget och hur ofta.
- Även om slutgiltig pseudonymisering ska ske automatiskt, gå manuellt igenom listan över personer som markerats för pseudonymisering under den första tiden för att säkerställa att urvalet passar er verksamhet.
- När ni hittat rätt inställningar behöver ni fortfarande kontrollera listan med någon veckas intervall (ej över 30 dagar) för att säkerställa att funktionen fungerar ordentligt.

Gallring

Information

I direktivet beskrivs hur pseudonymisering och gallring kan användas för att inte uppgifter ska lagras längre än nödvändigt. Personuppgifter kan gallras manuellt. Vi har valt att initialt fokusera på pseudonymisering eftersom gallring av bokningar, köp, besök med mera kraftigt skulle begränsa följande funktioner:

- Försäljningsstatistik
- Servicegrad vid återköp och reklamationer (där Registrerads koppling till bokning och köp möjliggör hantering trots att han/hon inte sparat kvittot).
- Besöksstatistik (som behövs för att planera bemanning under året)
- Besöksloggar (som är nödvändiga pga säkerhet i händelse av incidenter och för felsökning när kunder rapporterar problem)
- Träningsstatistik (som presenteras för slutkund / registrerad person)

Kommunikation med tidigare registrerade personer (tillval)

Information

Om ni bedömer det vara förenligt med GDPR (intresseavvägning) kan ni aktivera en funktion som vid pseudonymisering överför personens e-postadress till ett externt e-postsystem, exempelvis MailChimp. På så sätt kan ni informera kunder om era tjänster trots att personen inte längre är registrerad i Systemet.

Ny funktionalitet

- Inställning som aktiverar funktionen
- Vid pseudonymisering, lägg personens e-postadress till lista i externt e-postsystem, exempelvis MailChimp, förutsatt att "Tillåt massutskick via e-post" är aktiv.

Rutiner

Om funktionen aktiverats och det vid markering för pseudonymisering finns skäl till att inte överföra personen till ett ett externt e-postsystem, inaktivera "Tillåt massutskick via e-post".

Slutet system för spärrade personer (tillval)

Information

Även personer som inte betalat sina skulder eller fått anmärkningar på grund av beteende som strider mot avtalet har rätt att pseudonymiseras. Personuppgiftsansvarig kan då välja att lägga personen till ett slutet system som kan fungera som verktyg för att hindra dessa kunder från att åter registrera sig som kunder.

Ny funktionalitet

- Inställning som aktiverar funktionen.
- Rättighet som avgör vilka användare som får markera personer som spärrade
- Möjlighet att markera en person som spärrad
- Vid pseudonymisering av spärrad person, lägg personen till det slutna systemet.
- Rättighet som avgör vilka användare som får tillgång till det slutna systemet
- Möjlighet att permanent radera personer från listan över spärrade personer
- Vid försök att registrera en person, matcha automatiskt telefon och personnummer (Sverige) mot listan och hindra vid träff registrering med hänvisning till spärrlista.
- Vid försök till registrering via internetbokning (generation 2), hindra på samma sätt registrering och be användaren kontakta personal på anläggningen.

Rutiner

Fastställ en tydlig policy där det framgår när ni spärrar en person. Överväg att informera om policy i avtalet. Ge endast ett fåtal personer tillgång till listan över spärrade personer.

Information om registrerade personuppgifter (basfunktionalitet)

Information

Registrerade personer ska enkelt få tillgång till information om vilka personuppgifter som normalt registreras och hur de används.

Ny funktionalitet

- Ny meddelandemall "Personuppgiftspolicy" där personuppgiftsansvarig själv kan formulera sin policy.
- Visa personuppgiftspolicy i internetbokningen (generation 2).

Rutiner

Formulera en tydlig policy där det framgår vad som registreras och hur uppgifterna används.

Utdrag från personregister (tillval)

Information

En registrerad person som begär ett utdrag av vad som registrerats har rätt till detta. Eftersom det är viktigt att informationen endast lämnas ut till den registrerade personen och ingen annan behöver Registrerad besöka anläggningen så att identifiering är möjlig.

Ny funktionalitet

- Inställning som aktiverar funktionen. Annars kan personal på anläggningen själv sammanställa den manuellt vilket tar längre tid men ger större möjlighet till att välja vad som ska följa med.
- Inställningar som avgör vad som ska ingå i utdraget beroende på hur personuppgiftsansvarig tolkar direktivet.
- Rättighet som avgör vilka användare som får skapa ett utdrag från personregister.
- Möjlighet att markera en person och skapa en fil som innehåller ett utdrag utifrån de inställningar som gjorts.
- Loggas att utdrag skapats.

Rutiner

Skapa en rutin för hur en person som begär utdrag från personregistret ska identifiera sig, vem som gör utdraget, vilken information utdraget ska innehålla och om informationen ska överlämnas direkt på plats eller efter ett antal dagars väntetid.

Hantering av barns personuppgifter (basfunktionalitet)

Information

Om ett barn är under 16 år är behandling av personuppgifter endast tillåten om föräldern ger samtycke. Barn förekommer i systemet som deltagare på arrangemang (exempelvis simskolor) där beställaren är en förälder, eller som registrerade personer för exempelvis abonnemang eller tjänstebokningar.

Normalt är det enda fält som behövs vid beskrivning av arrangemangsdeltagaren för och efternamn vilket är nödvändigt för att tjänsten ska kunna levereras. Om kontroll av minimiålder (inställning) aktiverats för arrangemanget frågar internetbokningen även efter barnets födelsedatum för ålderskontroll. Detta sparas endast i loggen som hjälp om det visar sig att föräldern lämnat felaktiga uppgifter.

Ny funktionalitet

- Gör det möjligt att genom systeminställning aktivera "Kräv att arrangemangsdeltagare har en personkoppling" utan att deltagarens personnummer måste uppges.
- Gör det möjligt att genom systeminställning aktivera ålderskontroll för arrangemang med endast födelsedatum - inte personnummer (endast Sverige).
- När en person under 16 års ålder (systeminställning) registreras I de förenklade kundrutinerna eller från personlista, be om förälders samtycke och logga tidpunkt för godkännade och referens till anställd.
- När en person under 16 års ålder registreras i kundwebben (generation 2), be om förälders samtycke och logga tidpunkt för godkännade och kanal (internetbokning).

Rutiner

- Konfigurera ålderskontroll och personkoppling för arrangemang på ett sätt som ni bedömer är förenligt med GDPR.
- Avgör om ni bedömer att registrering av barnets förnamn, efternamn och eventuellt födelsedatum i samband med att föräldern ingår ett avtal vid köp av tjänsten är förenligt med GDPR.
- Utforma rutin för att inhämta samtycke när barn registreras i receptionen.

Rätt till invändning

Information

Registrerad person har rätt att invända om registrering eller behandling av personuppgifter skett utan avtal eller samtycke.

Rutiner

Vid invändning från registrerad, rätta eller pseudonymisera registrerad information.

Personer som registrerats innan GDPRs inträde

Information

Om ni gjort ändringar i avtalet i samband med GDPR har tidigare registrerade personer inte läst eller godkänt dessa.

Rutiner

Bedöm om ni anser att ni med hänvisning till intresseavvägning kan välja att endast genom utskick och skyltar på anläggningarna informera om det nya avtalet och er personuppgiftspolicy, eller om ni behöver inhämta godkännande från samtliga registrerade personer.

Rätt till rättning (basfunktionalitet)

Information

Registrerad person har rätt att lämna nya uppgifter om de som registrerats inte stämmer, exempelvis om namn eller adress är felaktiga.

Ny funktionalitet

- Möjlighet att överrida personuppslagning för vissa fält.

Rutiner

- Vid begäran om rättning, korrigera felaktig information.
- Om personuppgifter exporteras till andra system, gör ändringen där med. Hela kedjan ska informeras om det inte är för betungande.

Rätten att bli bortglömd

Information

Begäran om radering måste ha en grund, exempelvis att samtycke saknas. Förfrågan hanteras på anläggningen eftersom bedömning av personal och ID-kontroll behöver göras.

Rutiner

- Kontrollera ID
- Säg upp och slutbetala abonnemanget.
- Markera personen för pseudonymisering.
- Raderingen av personuppgifterna ska vara genomförda inom 30 dagar.

Dataportabilitet

Information

Omfattar bara information registrerad person matat in, exempelvis spellistor i Spotify. Ej profilering eller automatiskt registrerad information. Vi bedömer inte att denna typ av begäran är tillämpbar för den data som lagras i Systemet.

Automatiskt beslutsfattande

Information

Behöver bara begränsas om regler ger betydande påverkan för person. Vi bedömer inte att Systemet innehåller automatiska funktioner av denna typ.

Hantering av kontaktpersoner och leads

Information

Personer som inte är kunder eller anställda saknar avtal och har inte gett samtycke till registrering. Registrera endast dessa i systemet om ni bedömer att hanteringen kan vara tillåten med hänvisning till intresseavvägning.

Rutiner

- Utifrån er tolkning av GDPR, överväg att stänga av möjligheten att registrera sig i internetbokningen utan att genomföra en bokning.