Integritetsskydds myndigheten

Anmälan av personuppgiftsincident

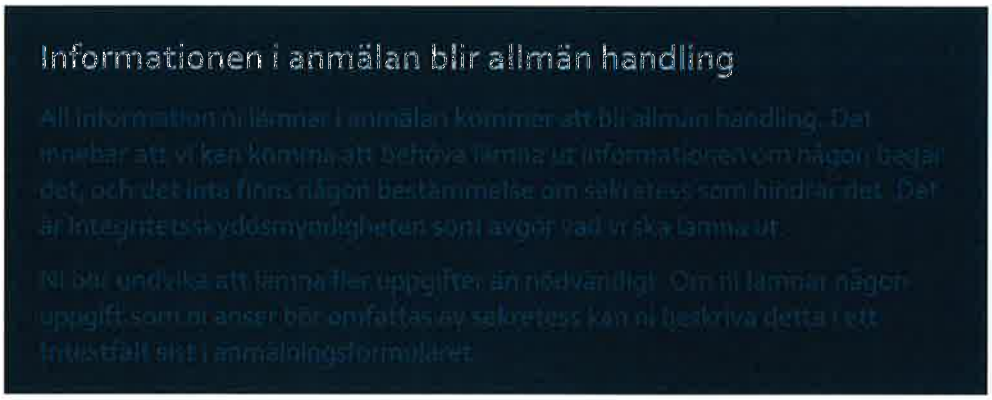
Använd den här blanketten för att anmäla en personuppgiftsincident som har inträffat i Sverige och inte påverkar registrerade personer i andra länder.

Fält med asterisk (*) är obligatoriska.

Komplettera anmälan
Det är möjligt att lämna kompletterande uppgifter i efterhand, men det är viktigt att vi får in informationen så fort som möjligt. Om ingen komplettering kommit in efter fyra veckor från det att vi tagit emot anmälan fattas beslut i ärendet på befintlig information.

Läs mer om personuppgiftsincidenter på vår webbplats www.imy.se/pui.

På vår webbplats finns också information om hur Integritetsskyddsmyndigheten hanterar personuppgifter.



Personuppgiftsansvarig

1. Organisationens namn *	Skriv namnet på den personuppgiftsansvarige där incidenten har inträffat.
Bostads AB Poseidon	
2. Organisationsnummer	Ange organisationsnummer (XXXXXX-XXXX). Obs! Om den personuppgiftsansvarige är en enskild firma ska detta fält inte fyllas i.
556120-3398	
3. Organisationens postadress *	Ange postadress (det vill säga inte besöksadress).
Bostads AB Poseidon Box 1 424 21 ANGERED	
4. Er organisations interna referensnummer	Ert referensnummer för egen uppföljning.

Kontaktuppgifter för anmälan

5. Kontaktpersonens namn *	Namnet på den som vi kan kontakta.
Sofia Björkled	
6. Kontaktpersonens roll Markera endast ett alternativ.	
☐ Dataskyddsombud ■ Annan roll	
7. Kontaktpersonens e-post*	
sofia.bjorkled@poseidon.goteborg.se	
8. Kontaktpersonens telefonnummer *	
031-3321006	
9. Den adress ni önskar bli kontaktad på *	Brev som vi skickar till er gällande anmälan kommer att skickas till den här adressen.
Bostads AB Poseidon Box 1 424 21 ANGERED	

Incidenten	
10. När inträffade incidenten? 2023-04-24	Ange datum och klockslag (ÅÅÅÅ-MM-DD HH:MM) och eventuell kommentar.
11. När upptäckte ni incidenten? 2023-04-25	Ange datum och klockslag (ÅÅÅÅ-MM-DD HH:MM) och eventuell kommentar.
12. Pågår incidenten fortfarande? ■ Ja ☐ Nej Om ni svarat *ja* på frågan ovan, gå till fråga 14.	
13. När upphörde incidenten?	Ange datum och klockslag (ÅÅÅÅ-MM-DD HH:MM) och eventuell kommentar.

14. Om er anmälan kommer in senare än 72 timmar efter att ni upptäckte incidenten, beskriv varför.

Eftersom tjänsten där incidenten inträffat är en så kallad kommungemensam tjänst där Göteborgs stads nämnd för intraservice är leverantör har Poseidon inte själva haft kontakt med den drabbade leverantören utan all information har gått via nämnden för intraservice. Informationen har hela tiden indikerat att ingen information har stulits men att utredning pågår. Poseidons initiala bedömning har då varit att det är osannolikt att personuppgiftsincidenten medför risk för fysiska personers fri- och rättigheter och att incidenten därför inte behöver anmälas till tillsynsmyndigheten men att händelsen ska fortsätta övervakas om det blir aktuellt med rapportering. Nu har ytterligare information getts som gör att vi inte längre kan se det som osannolikt att incidenten medför risk för fysiska personers fri- och rättigheter. Av den anledningen anmäls incidenten först nu.

15. Vad har hänt vid incidenten?
Markera endast *ett* alternativ.

Välj det alternativ som stämmer bäst överens med det som inträffat.

- ☐ Obehörigt röjande genom felaktigt utskick av mejl/brev/sms
- ☐ Obehörigt röjande: Övrigt
- ☐ Obehörig åtkomst: Någon inom eller utanför organisationen har tagit del av information som den saknade behörighet till
- ☐ Förlust: Information har gått förlorad på något sätt, till exempel genom att en dator blivit stulen
- ☐ Förstöring: Någon eller något har förstört information, till exempel genom att en dator har gått sönder
- ☐ Ändring: Personuppgifter har ändrats på något sätt

16. Kort beskrivning av incidenten

Visma Recruit är en gemensam tjänst för staden. All information har därför nått oss genom nämnden för intraservice som är vår leverantör av tjänsten.

Måndag eftermiddag, 24 april får Visma information av en av deras driftleverantörer, Iver, att deras datacenter i Stockholm var offline pga driftproblem, vilket innebar att ett av våra rekryteringssystem, Visma Recruit, var lagel offline.

Tisdag 25 april får Visma indikationer från Iver att det handlar om en cyberattack och att de lagrt ner sin miljo som en proaktiv åtgärd. Iver har inga indikationer på att data exponerats eller har gått förlorad.

Torsdag 27 april. Iver konfirmerar att Vismas servrar har krypterats med ransomware men det finns inga tecken på att data har blivit stulen

Fredag 28 april. Visma informerar om att inskickade ansökningar och bilagor uppladdade mellan sista backup och när tjänsten stängdes har gått förlorade.
Bilagor mellan lördag 00.01 och måndag 06.00 har gått förlorad.
För data utöver bilagor gäller tiden måndag 00.01 - 06.00.
Visma informerar om att de ska göra riktade informationsutskick till de som sökt tjänster under den perioden där de ombads ladda upp informationen på nytt.

Måndag 1 maj. Visma recruit är uppe igen efter att ha återställts med backup.

Onsdag 4 maj. Poseidon HR-chef i samråd med dataskyddskonlaklen bedömer med den samlade information som hittills nått oss från nämnden for intraservice att det är osannolikt att personuppgiftsincidenten medför risk för fysiska personers fri- och rättigheter och att incidenten därför inte behöver anmälas till tillsynsmyndigheten

Onsdagen 10 maj
Vid bolagets GDPR-möte resonerar gruppen kring incidenten. Då ingen ytterligare information erhållits görs bedömningen att incidenten inte ska anmälas till IMY.

Torsdag 11 maj
Intraservice går ut med ett nytt utskick där de anger att det finns en risk att personuppgifter blivit obehörigt röjda. Med den nya informationen ses det inte längre som osannolikt att personuppgiftsincidenten medför risk för fysiska personers fri- och rättigheter och incidenten behöver därför rapporteras till tillsynsmyndigheten. Det finns fortsatt ingenting som indikerar att personuppgifter har stulits men servicleverantören kan inte heller garantera att så inte är fallet. Bolaget beslutar att anmäla incidenten.

17. Hur upptäckte ni incidenten?
Markera endast *ett* alternativ.

- ☐ Genom en automatiserad process: Tekniska säkerhetsåtgärder
- ☐ Genom organisatoriska rutiner, till exempel en återkommande kontroll
- ☐ En anställd informerade oss
- ■ Vårt personuppgiftsbiträde informerade oss
- ☐ En utomstående eller registrerad informerade oss

18. Varför inträffade incidenten enligt er uppfattning?
Markera endast *ett* alternativ.

- ☐ Mänskliga faktorn: Fel i det enskilda fallet
- ☐ Brist i organisatoriska rutiner eller processer: Systematiska fel
- ☐ Tekniskt fel, till exempel fel i mjukvara, programinställningar
- ☐ Medvetet angrepp från någon i organisationen
- ■ Antagonistiskt angrepp: Angrepp utifrån
- ☐ Okänd orsak
- ☐ Övrigt:

19. Inom vilken sektor inträffade incidenten?
Markera endast *ett* alternativ.

- ■ Offentlig sektor
- ☐ Privat sektor
- ☐ Övrigt

20. Inom vilket verksamhetsområde inträffade incidenten?
Markera endast *ett* alternativ.

- ☐ Hälso- och sjukvård
- ☐ Socialtjänst
- ☐ Skola: Förskola, grundskola, gymnasium
- ☐ Universitet eller högskola
- ☐ Annan eftergymnasial utbildning
- ☐ Forskning
- ☐ Finansiell sektor eller försäkring
- ☐ Kreditupplysning
- ☐ Inkasso
- ☐ Näringslivet i övrigt
- ☐ Polis
- ☐ Rättsväsendet i övrigt
- ☐ Ideell organisation eller ekonomisk förening
- ■ Kommun
- ☐ Statlig myndighet
- ☐ Övrigt:

Biträden

21. Gäller incidenten en personuppgiftsbehandling som hanteras av anlitade personuppgiftsbiträden eller underbiträden?

- [x] Ja
- [ ] Nej

Om ni svarat *nej* på frågan ovan, gå till fråga 23.

22. Organisationens namn och organisationsnummer.

Organisationens namn: Nämnden för intraservice

Organisationsnummer:

Organisationens namn: Visma Talent Solutions AB

Organisationsnummer: 556613-1636

Organisationens namn: Iver Sverige AB

Organisationsnummer: 556575-3042

Uppgifterna och de registrerade

23. Hur många registrerade har påverkats?

Exakt antal registrerade:

Om ni inte känner till det exakta antalet kan ni uppskatta antalet genom att fylla i något av de angivna intervallen. Markera endast *ett* alternativ.

- ☐ 1–10
- ☐ 11–100
- ☐ 101–1 000
- ☐ 1 001–10 000
- ☐ 10 001–100 000
- ☐ 100 001–500 000
- ☐ 500 001–1 miljon
- ☐ Över 1 miljon
- ■ Okänt/kan inte ange

24. Hur många uppgifter om de registrerade har påverkats totalt?

Exakt antal uppgifter:

Om ni inte känner till det exakta antalet kan ni uppskatta antalet och fylla i något av de angivna intervallen. Markera endast *ett* alternativ.

- ☐ 1–10
- ☐ 11–100
- ☐ 101–1 000
- ☐ 1 001–10 000
- ☐ 10 001–100 000
- ☐ 100 001–500 000
- ☐ 500 001–1 miljon
- ☐ Över 1 miljon
- ■ Okänt/kan inte ange

25. Vilka grupper tillhör de registrerade?
Markera *alla* alternativ som gäller.

- [x] Anställda hos den personuppgiftsansvarige
- [ ] Användare av den personuppgiftsansvariges tjänster
- [ ] Kunder hos den personuppgiftsansvarige
- [ ] Prenumeranter
- [ ] Medlemmar, till exempel i en förening eller en kundklubb
- [ ] Militär, det vill säga anställda inom totalförsvaret
- [ ] Patienter
- [ ] Barn
- [ ] Skolelever i förskola, grundskola eller gymnasium
- [ ] Studerande i eftergymnasial utbildning
- [ ] Utsatta personer, till exempel personer som lever med skyddad identitet
- [ ] Övriga personer som enligt er bedömning drabbas särskilt hårt om personuppgifter sprids
- [ ] Kan inte ange för närvarande
- [x] Övrigt:

26. Vilken sorts personuppgifter har incidenten drabbat?
Markera *alla* alternativ som gäller.

- ☐ Etniskt ursprung
- ☐ Politiska åsikter
- ☐ Religiös eller filosofisk övertygelse
- ☐ Medlemskap i fackförening
- ☐ Genetiska uppgifter
- ☐ Biometriska uppgifter
- ☐ Hälsa
- ☐ Sexualliv eller sexuell läggning
- ☐ Uppgift om brott
- ☐ Personnummer
- ☐ Ekonomisk eller finansiell information
- ■ Officiella dokument
- ☐ Lokaliseringsuppgifter (till exempel GPS-position, ej adressuppgifter)
- ☐ Kommunikationsloggar
- ☐ Metadata om kommunikation
- ■ Identifierande information (till exempel för- och efternamn)
- ■ Kontaktinformation
- ☐ Okänd
- ☐ Övrigt:

27. Var personuppgifterna krypterade?
Markera endast *ett* alternativ.

- ☐ Ja, samtliga uppgifter
- ☐ Ja, men inte alla uppgifter
- ☐ Nej
- ■ Vet inte

Konsekvenser

28. Vad kan bli konsekvenserna av incidenten?
Markera *alla* alternativ som gäller.

- [x] Den registrerade förlorar kontrollen över de egna personuppgifterna
- [x] Begränsning av rättigheter
- [ ] Diskriminering
- [ ] Identitetsstöld eller bedrägeri
- [ ] Ekonomisk förlust
- [ ] Obehörigt hävande av pseudonymisering
- [ ] Skadat anseende
- [ ] Förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt
- [ ] Annan ekonomisk eller social nackdel
- [ ] Övrigt:

29. Hur allvarlig bedömer ni att incidenten är?
Markera endast *ett* alternativ.

Uppskatta hur allvarlig incidenten är med hänsyn till de registrerades integritet.

- [ ] 1. Obetydlig
- [ ] 2. Begränsad
- [ ] 3. Betydande
- [ ] 4. Mycket allvarlig

30. Hur har ni agerat efter incidenten?

Beskriv vad ni har gjort. Har ni vidtagit åtgärder eller avser att vidta åtgärder för att lösa problem, förebygga eller mildra effekterna av incidenten?

Ange datum och klockslag (ÅÅÅÅ-MM-DD HH:MM)

Datum och klockslag: 24-04-2023 - 02-05-2023

Åtgärd:

Se Incidentrapport för åtgärder som Visma Talent Solutions har utfört under perioden. Bifogas.

Datum och klockslag: 04-05-2023 12:00

Åtgärd:

Visma Talent Solutions gör ett generellt utskick till alla som sökt en roll hos Poseidon mellan den 22/4 00.01 - 24/4 00.03 med uppmaning om att ladda upp sina bilagor på nytt.

Datum och klockslag:

Åtgärd:

Datum och klockslag:

Åtgärd:

Information till de registrerade

31. Har ni informerat de registrerade om incidenten?
Markera endast *ett* alternativ.

- ☐ Ja
- ■ Nej

Om ni svarat *nej* på frågan ovan, gå till fråga 33.

32. När informerade ni de registrerade?

Ange datum (ÅÅÅÅ-MM-DD)

Datum:

Gå till fråga 36.

33. Kommer ni att informera de registrerade?
Markera endast *ett* alternativ.

- ☐ Ja
- ☐ Nej
- ■ Vi har inte tagit ställning än

Om ni svarat *nej* eller *vi har inte tagit ställning än* på frågan ovan, gå till fråga 35.

34. När kommer ni att informera de registrerade?

Ange datum (ÅÅÅÅ-MM-DD)

Datum:

Gå till fråga 36.

35. Varför kommer ni inte att informera de registrerade?
Markera *alla* alternativ som gäller.

- ☐ Incidenten medför inte hög risk för personers fri- och rättigheter
- ☐ Personuppgifterna var krypterade eller på annat sätt skyddade
- ☐ Vi har redan vidtagit åtgärder som avhjälper riskerna
- ☐ Att informera innebär en oproportionell ansträngning, vi har istället informerat allmänheten

Komplettering/eventuell sekretess

36. Avser ni att komplettera er anmälan?
Om ni ska komplettera anmälan så måste det ske skyndsamt.
Markera endast *ett* alternativ.

- [x] Ja
- [ ] Nej

37. Om ni anser att viss information i er anmälan bör omfattas av sekretess, beskriv vilken information som enligt er bör vara sekretessbelagd och varför.

Har du frågor?

Läs mer om personuppgiftsincidenter på vår webbplats www.imy.se/pui

Om du inte hittar svaret där kan du kontakta oss på personuppgiftsincidenter@imy.se eller per brev.

Kontakt

Integritetsskyddsmyndigheten
Box 8114
104 20 Stockholm

Bilaga till incidentrapport

Bedömning 03-05-2023
Då det inte finns några indikationer på att personuppgifter blivit stulna under incidenten utan att det endast handlar om att de varit otillgängliga så bedöms det inte ha påverkat de registrerade negativt. Rekryteringsprocessen har pausats under nertiden och förutsättningarna för att söka och få arbete på Bostadbolaget har inte påverkats. I de fall där uppgifter har förlorats har utskick gått ut för att ge personerna chansen att åter ladda upp materialet.
Bostadsbolaget bedömer att incidenten inte behöver anmälas till IMY, då incidenten inte bedömts troligt medföra en risk för personens fri- och rättigheter.

Omvärderad bedömning 10-05-2023
Intraservice går ut med ett nytt utskick där de anger att det finns en risk att personuppgifter blivit obehörigt röjda och att angriparna hotar den utsatta serverleverantören med att läcka ut stulna uppgifter om inte en lösensumma betalas. Med den nya informationen ses det inte längre som osannolikt att personuppgiftsincidenten medför risk för fysiska personers fri- och rättigheter och incidenten behöver därför rapporteras till tillsynsmyndigheten.

iver

Incident

Nedanstående text baseras på information känd för Iver 2023-04-26 kl. 14.30. Uppdateringar för kommande datum och klockslag längre ned i dokumentet.

Bäste kund,

Tidigt på morgonen den 24 april drabbades Iver av ett intrång i en begränsad miljö. Det rör sig om ett begränsat cyberangrepp på en infrastruktur hos Iver. I den miljö som är drabbad av incidenten finns flera kunder. Vi utgår från att alla kunder i den drabbade miljön också är drabbade av säkerhetsincidenten. Den drabbade miljön finns i Sverige.

Cyberangreppet är alltid allvarliga och Iver tar angreppet på största allvar. Detta får konsekvensen att system för kunder i den drabbade miljön är otillgängliga till dess att vi med säkerhet kan säga att det är säkra igen och att ingen utomstående har åtkomst till några system.

Ivers *krisledningsgrupp* är aktiverad sedan morgonen måndag den 24 april. Ivers *Cyber Incident Respons Team* arbetar sedan krisledningsgruppens aktiverats dygnet runt med alla resurser som krävs för att kartlägga omfattningen av angreppet och säkerställa säkerheten och integriteten i miljön. I första skedet arbetar gruppen med att begränsa omfattning och undersöka skadan. När den grundläggande infrastrukturen är säkrad övergår vi till att återställa och "tvätta" system för att säkerställa att de inte bär några spår av angreppet innan de åter kan sättas i produktion.

För att återställa funktionaliteten i system innan de åter sätts i produktion behöver ett antal åtgärder vidtas. Detta innefattar uppgifter så som installation av EDR, patcha och gå igenom privilegierande behörigheter i systemet. Syftet med detta är att säkerställa att det inte finns några spår av skadlig kod på systemet och att systemet inte är sårbart på något annat sätt som äventyrar säkerheten eller integriteten i systemet. När detta är säkerställt kommer vi kontakta er för att säkerställa funktionalitet i systemen.

Alla cyberangrepp riskerar att också innebära en *personuppgiftsincident*. Detta beror dels på omfattningen av angreppet, dels den information som ni som kund lagrar och bearbetar i systemen. Vi ber er som kund att analysera vilken typ av information som ni har lagrar i miljöerna. Ert kundteam på Iver har också vägledning kring vilka faktorer som ska beaktas i bedömningen huruvida det riskerar att röra sig om en personuppgiftsincident eller inte.

Du som drabbad kund ska ha en etablerad dialog med er kundansvarige på Iver om incidenten. Vi ser gärna att du som kund ger er kundansvarige på Iver information om vilka av era system som ej är nåbara nu som är mest kritiska för er. De mest kritiska systemen för er är de vi kommer att prioritera först när system efter system åter sätts i produktion och då kommer vi också behöva er hjälp att verifiera funktionalitet i dessa.

Det finns en risk att även klienter som är direkt anslutna till AD i drabbad miljö kan vara påverkade. Har ni klienter som är anslutna direkt till denna miljö kommer vi att kontakta er för att hantera detta. Klienterna kommer inte kunna återansluta till miljön innan vi säkerställt att det kan göras på ett säkert sätt. Misstänker ni att klienter är drabbade, isolera dem (dra ur nätverkssladd, isolera från wifi) så att datorn inte kan kommunicera med omvärlden.

iver

Vi kan just nu inte ge ett bra estimat för när ni som kund återigen kan ha tillgång till era system och tjänster. Vi gör just nu allt vi kan för att "tvätta" och återställa kritisk infrastruktur. Parallellt förbereder vi naturligtvis också för återställning av system.

Med vänlig hälsning

Jesper Blomé
Head of Security & Compliance
Iver

Uppdatering 2023-04-26 kl. 22.00

Med information känd just nu är det sannolikt att intrånget startade något tidigare än vad vi informerat om i föregående version, sannolikt någon gång mellan kl. 23.00 den 23 april och klockan 00.00 den 24 april.

Uppdatering 2023-04-27 kl. 08.30

Fortsatt arbete har pågått under hela natten till idag med bra framdrift. Vi har nu mer infrastruktur på plats för att fortsätta återskapande av tjänster. Parallellt pågår återläsning och "tvätt" av kundsystem.

Uppdatering 2023-04-27 kl. 09.30

Alla cyberangrepp riskerar att också innebära en personuppgiftsincident. Detta beror dels på omfattningen av angreppet, dels den information som ni som kund lagrar och bearbetar i systemen. Vi ber er som kund att analysera vilken typ av information som ni har lagrar i miljöerna.

Vår preliminära bedömning av situationen nu är att risken för att detta är en incident som leder till risker för de registrerades fri- och rättigheter är reell. Vi rekommenderar därför att ni, utan dröjsmål, som personuppgiftsansvarig gör en anmälan till tillsynsmyndigheter (IMY) som ni sedan kan komplettera med ytterligare information.

iver

Iver Sverige AB
556575-3042

Evenemangsgatan 2C, Solna
Box 1476, SE 171 28 Solna

+46 8 506 106 00
info@iver.se

www.iver.se