dataskydd.net
ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Malmö 2017-06-05

Konsekvensbedömning avseende dataskydd – för Dataskydd.net

I enlighet med Dataskyddsförordningens artikel 35 har Dataskydd.net gjort en konsekvensbedömning av personuppgiftsbehandling vi genomför eller riskerar att genomföra genom vår verksamhet. Vi tror att konsekvensbedömningen gör det lättare för den som vill att förstå hur vi hanterar personuppgifter och på vilka sätt vi dataminimerar (enligt förordningens artikel 5.1.c). Konsekvensbedömningen är framtagen tillsammans med medlemmarna genom föreningens plattform Mattermost, och sammanställd av ordföranden.

Övergripande risker

De uppgifter privatpersoner i olika sammanhang lämnar hos oss är e-postadresser, pseudonymer (eller egennamn) samt chattloggar. Föreningen har också under sitt projekt Webbkoll/Kommunundersökning hanterat faktureringsuppgifter från två medlemmar (ordförande och kassör).

Chattloggar genereras av medlemmar. E-postadresser kan däremot komma att lämnas in till föreningen av en bredare grupp individer, även de som inte är medlemmar. Till exempel när man prenumererar på nyhetsbrev.

Medlemskap i föreningen

För att lösa medlemskap i föreningen måste man betala in medlemsavgiften och ge föreningen något sätt att koppla betalningen till en själv. Som ”koppling” godtar föreningen att man uppger en e-postadress och/eller en pseudonym (nick, smeknamn) i samband med inbetalningen.

I praktiken behöver man uppge en e-postadress (ett sätt för föreningen att kontakta medlemmen) för att kunna utöva sina rättigheter som medlem. När vi tar emot inbetalningar via bankgiro har det också varit fallet att föreningens kassör får tillgång till varje betalande medlems för- och efternamn.

Det är ett implicit krav för att kunna delta på årsmöten från föreningen sida att man kan använda Dataskydd.net:s kommunikationsverktyg Mattermost (se längre ned). Då krävs inloggning med e-postadress. Inuti Mattermost kan man välja en ny pseudonym, som inte behöver vara samma som den som är kopplad till ens betalning, men som måste vara unik i förhållande till föreningens andra medlemmar.

För att kunna lämna in motioner till årsmötet finns inget krav utöver att man kan kontakta föreningen på ett sätt som går att koppla till en inbetalning.

Sedan 2017 skriver vi bara in pseudonymer i årsmötesprotokollet om inte medlemmen specifikt vill beskrivas med det egennamn som staten betecknar individen med i sin förvaltningsverksamhet.

Medlemsregister

Medlemsregistret finns i dagsläget på kassörens privata dator. Det är en krypterad CSV-fil som innehåller medlemsnummer (används inte till något speciellt just nu), någon slags pseudonym (vanligtvis en e-postadress), samt datum för första/senaste/nästa inbetalning.

Att avsluta medlemskapet

När en person väljer att gå ur föreningen tas deras uppgifter/pseudonymer tas bort ur medlemsregistret (CSV-filen) inom en vecka. Vi tar också bort Mattermost-kontot och all där till hörande kommunikation (även skriftliga meddelanden gjorda i Mattermost), men ger medlemmen ett val om den även vill att dess skriftliga inlägg ska vara kvar trots avslutat medlemskap. Utträde ur föreningen och förlust av medlemskap sker om medlemmen anger att den vill gå ur föreningen eller om den inte betalar in sin medlemsavgift.

Om medlemmen även är prenumerant på nyhetsbrevet kan den själv avprenumerera. Då försvinner e-postadressen ur utskickslistan.

Prenumeration på nyhetsbrev

För att prenumerera på nyhetsbrevet behöver man uppge sin e-postadress. E-postadresser kan ibland innehålla mer personuppgifter än vad en person tänker sig: dels kan det förekomma egennamn i e-postadressen, dels kan e-postadressen ge uppgift om var man arbetar eller vilken personlig webbplatsadress man har.

Listan med e-postadresser som prenumererar på nyhetsbrevet är tillgänglig i Dataskydd.net:s webbplatsplattform (se nedan), och går att läsa av personer som kan redigera webbplatsens innehåll och har administratörsrättighet. Administratörsrättigheter innehas för närvarande av två personer: ordföranden och kassören.

Om man slutar prenumerera på nyhetsbrevet tas ens e-postadress bort ur listan av prenumeranter. Den slutar då vara tillgänglig för redigerare på webbplatsen med administratörsrättigheter.

Dataminimering

För att i så hög utsträckning som möjligt minska våra besökares, medlemmars och prenumeranters exponering mot informationssäkerhetsrisker lagrar vi så lite data som möjligt. Våra medlemmar behöver vara identifierade bara i den utsträckning att de kan skiljas från varandra vid årsmöten, och en prenumerant behöver bara en fungerande e-postadress (som inte behöver vara kopplad till någon personlig information). Vi har inga webbanalysverktyg och använder heller inga webbkakor av samma skäl.

Vid bankgiroöverföringar får föreningens kassör ta del av betalningsutförarens förnamn och efternamn eftersom sådan information skickas med av banken vid bankgiroöverföringar.

Rutiner för att underrätta medlemmar om säkerhetsproblem

Om Dataskydd.net drabbas av en personuppgiftsincident har vi företrädelsevis två vägar att kommunicera detta till berörda privatpersoner. Vi kan använda utskickslistan för nyhetsbrevet, eller kommunikationsinstansen Mattermost. Vi kan också kombinera dessa.

Vi följer de tio gyllene reglerna för incidenthantering som beskrivs i IT-kommissionens rapport 39/2001.[1]

Mjukvaruplattformar och tredjeparter

Webbplatsplattform

Dataskydd.net:s nuvarande (2017) webbplatsplattform är Drupal. Vi har inga webbanalysverktyg och lagrar inte heller IP-adresser från de som besöker webbplatsen.

Personuppgifter lagras i plattformen för de som kan redigera webbplatsens innehåll. Dessa personuppgifter utgörs av e-postadress, pseudonym och egennamn (frivilligt), Redigerarna ansvarar själva för att sätta ett lösenord som skyddar deras och andras personuppgifter.

Personer som kan redigera webbplatsen tillhör en av flera behörighetsnivåer, där samtliga behörighetsnivåer inte har samma tillgång till alla uppgifter i systemet.

Uppdateringsrutiner: Dataskydd.net uppdaterar Drupal samma dag när det släpps nya säkerhetsuppdateringar.

Kommunikationsverktyg

Dataskydd.net har en intern kommunikationsinstans i form av Mattermost, en webbtjänst som liknar Slack men som går att administrera på egna servrar.

Eftersom vi själva administrerar Mattermost behöver vi inget extra avtal med en extern tjänsteleverantör utan vi är i princip ensamt ansvariga för uppgifter i Mattermost.

För att vara med i Mattermost-instansen krävs att man är medlem i föreningar. Inloggningsuppgifterna utgörs av en e-postadress som medlemmen själv väljer och ett lösenord. I själva instansen får man en pseudonym (nick, smeknamn) som man själv får välja. Pseudonymet kan i princip vara ett egennamn men ingen medlem använder sitt egennamn som pseudonym just nu.

Uppdateringsrutiner: Dataskydd.net uppdaterar Mattermost så fort det släpps nya uppdateringar från utvecklarna (vanligtvis inom en dag).

[1] IT-kommissionen, Observatoriet för informationssäkerhet. PM 39:2001 *Hantering av IT-incidenter, vem gör vad och hur?* http://www.itkommissionen.se/doc/94.html

Serverplats och domäner

Dataskydd.net betalar för virtuella servrar hos Scaleway (en del av franska Online.net) i deras datacenter i Paris. Franska Gandi administrerar dataskydd.net:s domäner.

Vi har också tjänsten Webbkoll hos amerikanska Linode i London.

Föreningen sparar inga uppgifter om de som besöker våra webbplatser (t ex genom att lagra e-postadresser, kräva inloggning eller genom användning av webbanalysverktyg), men det finns en risk att besök till våra webbplatser plockas upp och kartläggs av statliga myndigheter i Storbritannien, Frankrike eller Sverige. Genom Linodes amerikanska verksamhet finns också exponering mot myndigheter i USA. Det bör i praktiken vara svårt för oss i dagsläget att tillhandahålla bättre skydd mot sådan kartläggning än vi redan gör, och slutanvändare är utelämnade åt att använda egna applikationer på sin egen dator (till exempel den anonymiserande webbläsaren Torbrowser) för att få ett starkare skydd.

Uppdateringsrutiner: Dataskydd.net är ansvariga för att hålla servrarna på Scaleway och Linode uppdaterade ur ett mjukvaruperspektiv; vi nyttjar Ubuntus funktion för automatiska säkerhetsuppdateringar. Scaleway och Linode är ansvariga för att upprätthålla en god säkerhetsnivå för sin egen infrastruktur.

Kommunikation med `info@dataskydd.net`-adressen

`info@dataskydd.net` vidarebefodras till två andra e-postkonton, ordförandens och kassörens. Det innebär att kommunikation och personuppgifter som skickas till info-adressen lagras i var och en av ordförandens och kassörens privata e-postlagringslösningar. Dataskydd.net har ingen egen mejl-server, utan bara adresser som pekar på andra e-postadresser.

Säkerhet

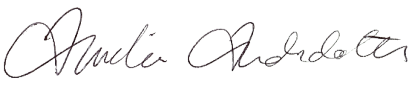
Kryptering

Vi har HTTPS på alla våra webbplatser för att uppgifter om hur man besöker vår webbplats ska vara skyddade från extern insyn. Vi använder kryptografiska certifikat från Let's Encrypt, som vi förnyar automatiskt en gång i månaden.

Medlemsregistret är också krypterat.

Vidarelämning av uppgifter

Vi lämnar inte vidare personuppgifter till tredjepart i annan utsträckning än vad som krävs för våra servrar. Vi lämnar inte heller ut personuppgifter till myndigheter annat än om myndigheten kan göra det sannolikt att att vi skulle drabbas av personliga eller ekonomiska sanktioner om vi lät bli.



Amelia Andersdotter
Ordförande, Dataskydd.net