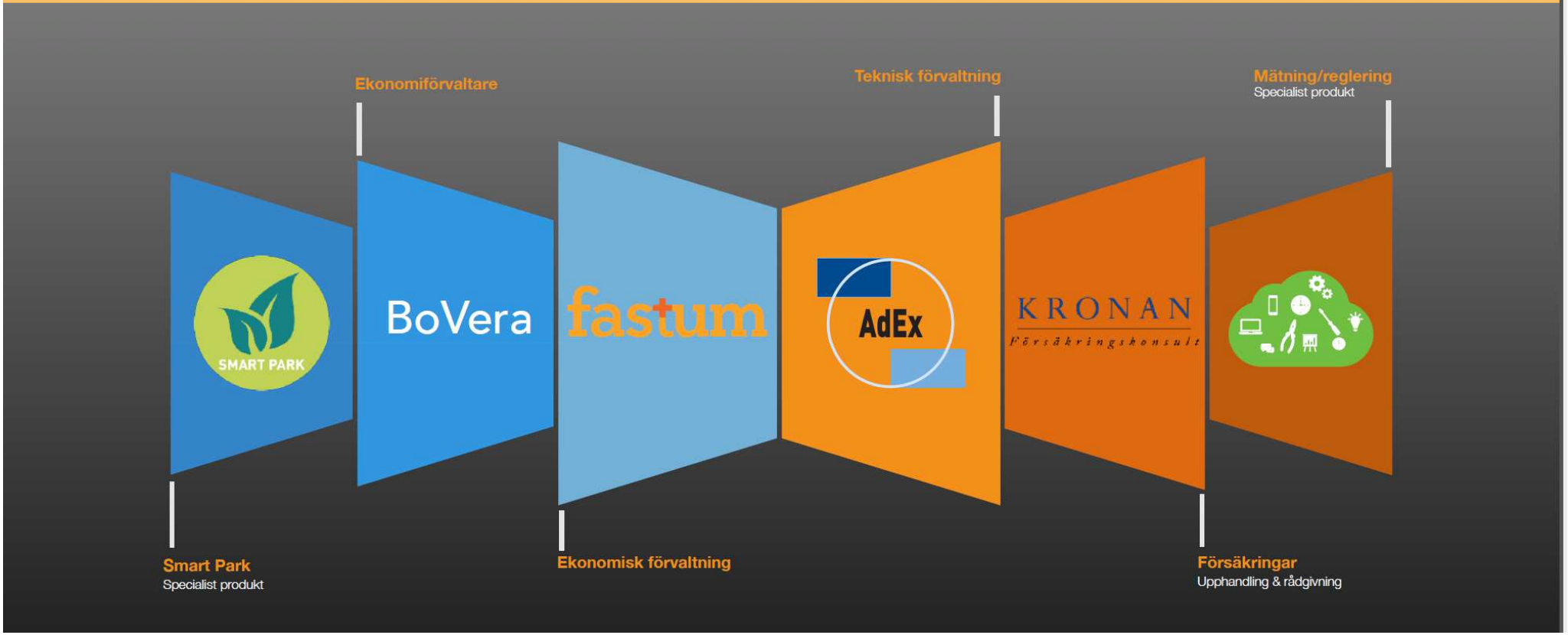
GRUPPEN fastum

SPECIALISTER I SAMVERKAN



Den nya dataskyddsförordningen

GDPR: Agenda

Introduktion och syfte

Begrepp

Nyheter i dataskyddsförordningen

Vad dataskyddsförordningen innebär för er som förening

Vilka åtgärder och förändringar som Fastumgruppen planerar för

GDPR: Introduktion

- Dataskyddsförordningen (GDPR) ersätter personuppgiftslagen (PuL)
- Den nya lagstiftningen träder i kraft den 25 maj 2018
- Direkt tillämplig i samtliga medlemsstater i EU

GDPR: Syfte

- Skydda människor från kränkning av den personliga integriteten
- Modernisering av reglering kring personuppgifter
- Ge individer ökad kontroll över sina personuppgifter
- Ökad harmonisering inom EU

GDPR: Begrepp

- **Personuppgift**

Varje upplysning som avser en identifierad eller identifierbar fysisk person (registrerad), som direkt eller indirekt kan identifieras. T ex namn, bild eller ljuduppgifter om en person, personnummer, IP-nummer.

- **Behandling**

En åtgärd eller kombination av åtgärder beträffande personuppgifter. Oavsett om de sker automatiserat eller inte. T ex insamling, lagring, bearbetning.

- **Personuppgiftsansvarig**

En person (fysisk eller juridisk) som bestämmer syftet med och medlen för behandling av personuppgifter. Ansvarar för att behandlingen är laglig och ska säkerställa att så är fallet.

- **Personuppgiftsbiträde**

En person (fysisk eller juridisk) som behandlar personuppgifter för den personuppgiftsansvariges räkning.

- **Samtycke**

Den registrerade godtar behandlingen av personuppgifter som rör den personen. Ska ske frivilligt, informerat och genom en tydlig viljeyttring (bekräftelse).

GDPR: Tillämpningsområde

- All helt eller delvis automatiskt behandling av personuppgifter
- Annan behandling av personuppgifter som ingår eller kommer ingå i ett register
- Inga undantag för ostrukturerad behandling av personuppgifter – missbruksreglen försvinner
- Verksamhet som bedrivs av en aktör som är etablerad i EU, oavsett om behandlingen utförs i EU eller inte

GDPR: Nyheter

- Gäller all behandling av personuppgifter
- Krav på aktivt samtycke
- Få tillgång till uppgifterna
- Flytt av data (dataportering)
- Rätt ”att bli glömd”
- Skyldighet att föra register över behandlingen
- Krav på att rapportera personuppgiftsincidenter
- Förbud mot att överföra personuppgifter till land utanför EU/EES
- Sanktionsavgifter vid överträdelser
- Krav på dataskydd (begränsa åtkomst och skydda uppgifterna samt anonymisera)
- Krav på gallring

GDPR: Personuppgiftsansvarig

- **Ansvar för hanteringen av personuppgifter**

Det är den personuppgiftsansvarige som ansvarar för korrekt hantering av personuppgifter

- **Säkerställa korrekt laglig grund för hanteringen av personuppgifter**

Exempel på laglig grund i för en förening finns i Lagen om ekonomisk förening och bostadsrättslagen samt i föreningens stadgar. Föreningen ska föra medlemsregister och lägenhetsförteckning utan att det ställs krav på samtycke.

- **Säkerställa tillräcklig säkerhet vid behandling**

Personuppgifterna måste förvaras på ett betryggande sätt. Gäller både tekniskt och organisatorisk. Dvs inte förvara personuppgifter så att obehöriga kan komma åt dem.

- **Föra register över vilka personuppgifter som behandlas och vart de behandlas**

Dock är mindre företag/organisationer undantagna från denna regel med vissa förbehåll. Ska sysselsätta färre en 250 personer. Rådet är att upprätta ett sådant register oavsett.

- **Lämna ut information – registerutdrag**

Ska lämna ut vilka uppgifter som finns registrerade om den person som frågar. Här ingår samtliga personuppgifter . Dvs även mail och worddokument.

GDPR: Vad är en personuppgift

”Information som direkt eller indirekt kan hänföras till en identifierbar fysisk person som är i livet.”

Artikel 4.1

GDPR: Kategorier av personuppgifter

Personuppgifter

- Namn
- E-post
- Födelsedatum
- IP-nummer
- Kakor
- MAC-adress
- Digitala fingeravtryck
- Pixel
- Beacons
- Loggar

Personuppgifter som *anses* vara känsliga

- Uppgifter om ekonomisk hjälp eller vård inom socialtjänsten
- Uppgifter om personliga och ekonomiska förhållanden inom bank- och försäkringsväsendet
- Uppgifter inom kreditupplysning eller inkassoverksamhet
- Personnummer

Känsliga personuppgifter*

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska och biometriska uppgifter
- Personuppgifter om hälsa
- Sexualliv eller sexuella läggning

*Behandlingen av känsliga personuppgifter är förbjudna enligt artikel 9. Kräver uttryckligen samtycke från den registrerade.

GDPR: Rättsliga grunder i en bostadsrättförening

Artikel 6

Samtycke (art 6 1.a)

E-postlistor
Facebook
Bilder

Avtal (art 6 1.b)

Medlemskap
Stadgar
Hyresavtal inklusive bilaga som reglerar personuppgifter

Rättslig förpliktelse (art 6 1.c)

Lagen om ekonomiska föreningar:
- Krav på medlemsregister

Bostadsrättslag:
- Krav på lägenhetsförtecknig

Årsredovisningslag:
- Formkrav på årsredovisning

Intresseavvägning (art 6 1.f)

Kameraövervakning
Passersystem
Tvättbokning
IP-adresser

GDPR: Exempel på känsliga personuppgifter

Andrahandsuthyrning

Att hyra ut i andra hand innebär att hyresgästen upplåter sin lägenhet till någon annan som ska använda lägenheten självständigt.

Man måste ha styrelsens samtycke för att få hyra ut sin lägenhet i andra hand samt att detta alltid är tidsbegränsat. Generellt rör det sig om tolv månader. Detta gäller också om man lånar ut lägenheten utan att ta ut någon hyra. Den som upplåter sin lägenhet utan lov riskerar att förlora den.

Föreningen kan inte neka den som har beaktansvärda skäl. Med beaktans exempelvis tillfälliga studier, arbete på annan ort, prova på sambo-boend på annan plats pga ålder eller sjukdom samt tillfälligt boende för vård av

Om styrelsen inte går med på en andrahandsupplåtelse av lägenheten, kan bostadsrättsinnehavaren överklaga hos hyresnämnden.

Skickas till styrelsen

Kräver uttryckligt samtycke

Bostadsrätt

Bostadsrättsförening	Lägenhetsnummer	Antal trappor

Adress	Postnummer	Ort

Lägenhetens användning	Antal rum	Yta i kvadratmeter
Lägenheten uthyres för att användas till bostad		

Till lägenheten hör			Nummer
☐ Källarutrymme	☐ Vindsutrymme	☐ Garageplats	

Skäl för andrahandsuthyrning

Tidsperiod för andrahandsuthyrning

Från och med - till och med	
	☐ Tills vidare

GDPR: Informationssäkerhet

Kategorier av personuppgifter

Säkerhetsåtgärder för vanliga personuppgifter

Säkerhetsåtgärder för känsliga personuppgifter

Personuppgifter

Personuppgifter som *anses* vara känsliga

Känsliga personuppgifter

Rättsliga grunder för vanliga personuppgifter

Rättsliga grunder för känsliga personuppgifter

GDPR: Exempel på hantering: Mäklarbild

Rättslig förpliktelse
Tex BRL 9 kap. 8 §

Bostadsrättsförening
PUA

Förvaltningsavtal
Biträdesavtal

Mäklare

Brf
innehavare

Avtal
Mäklaruppdrag

Beställer Mäklarbild

Ekonomisk förvaltare
PUB

Avtal - Förvaltningsavtal

Mäklarbild

Mäklare
PUA

Vi skickar mäklarbild till registrerad mäklare.
Efter 25 maj krävs tvåstegsverifiering

Mäklaren är ansvarig för personuppgiften

GDPR: Förslag på åtgärder

- Inventera vilka personuppgifter som föreningen har
- Upprätta ett register över föreningens personuppgifter
- Säkerställa att föreningen har laglig rätt till att hantera personuppgifterna
- Gör en åtgärdsplan för hur föreningen ska efterleva kraven i GDPR
- Upprätta avtal med föreningens respektive personuppgiftsbiträden

GDPR: Planerade åtgärder och förändringar

- **Nytt personuppgiftsbiträdesavtal**

För att säkerställa korrekt och laglig hantering av era personuppgift så krävs det ett nytt biträdesavtal för hanteringen av era personuppgifter. För att säkerställa kontinuiteten så garanterar Fastumgruppen lagring av föreningens bokföring och uppgifter under en period om 7 år efter respektive avslutad redovisningsperiod.

- **Register över samtliga personuppgifter**

För att säkerställa efterlevnad och möjligheten att snabbt skicka ut registerutdrag på eventuella förfrågningar gör Fastumgruppen en total genomgång av vilka personuppgifter som finns och hur de används.

- **Genomgång av den tekniska säkerhetsnivån**

I dialog med underleverantör säkerställs tillräcklig hög nivå av teknisk säkerhet.

- **Radering av gammal data**

Gäller dels gallring och radering av gamla system och e-post.

- **Nya arbetssätt**
  - Uppgifter som kräver högre informationssäkerhet hanteras med tvåstegsverifiering eller motsvarande (gäller tex UC, mäklarbrev,)
  - UC, mäklarbrev, etc skickas via Fastumdirekt eller länk. Ingen e-post ska användas

GDPR: Förslag på åtgärder

- Inventera vilka personuppgifter som föreningen har
- Upprätta ett register över föreningens personuppgifter
- Säkerställa att föreningen har laglig rätt till att hantera personuppgifterna
- Gör en åtgärdsplan för hur föreningen ska efterleva kraven i GDPR
- Upprätta avtal med föreningens respektive personuppgiftsbiträden

Se utdelad folder för mer information och besök gärna www.datainspektionen.se för mer information.

GRUPPEN fastum

SPECIALISTER I SAMVERKAN