GDPR-ANPASSA DIN VERKSAMHET

RÅD FÖR BEHANDLING AV PERSONUPPGIFTER

FASTIGHETSÄGARNA

Intresset av att kunna använda information om individer, så kallade personuppgifter, är stort i samhället. Som ett resultat av detta har skyddet för individers integritet blivit mer betydelsefullt.

INLEDNING

Den 25 maj 2018 ersattes tidigare gällande personuppgiftslagstiftning av en ny dataskyddsförordning (i dagligt tal GDPR – General Data Protection Regulation), som blev gällande lag i Sverige och övriga EU/EES.

Denna sammanställning syftar till att ge dig som medlem i Fastighetsägarna en introduktion till vad reglerna i GDPR innebär för din organisation och ge konkreta förslag till åtgärder som kan vidtas för att förbättra efterlevnaden av GDPR.

Sammanställningen är avsedd att fungera som ett hjälpmedel och komplement till annan information som du exempelvis kan erhålla från Datainspektionen och de vägledningar om personuppgiftsbehandling vid uthyrning av bostäder och vid kameraövervakning som tagits fram av Fastighetsägarna och SABO.

Är du osäker på om din organisation hanterar personuppgifter korrekt kan det vara klokt att även rådfråga en expert.

Denna skrift är framtagen mars 2017, reviderad oktober 2018.

GRUNDLÄGGANDE BEGREPP

Nedan presenteras vissa grundläggande begrepp som används i GDPR. Dessa begrepp är viktiga att förstå för att kunna kontrollera att din organisation följer de krav som finns i GDPR.

▶ PERSONUPPGIFTER
All slags information som antingen direkt eller indirekt (det vill säga via annan information) kan kopplas till en fysisk person, exempelvis namn, lägenhetsnummer, IP-adress, fotografier, ljudfiler, beteenden, preferenser, uppgifter om störningar, löneuppgifter och uppgifter om utbildning. De individer som din organisation behandlar personuppgifter om kan vara anställda, inhyrda konsulter, hyresgäster som är fysiska personer eller enskilda firmor, kontaktpersoner hos hyresgäster som är bolag, anställda hos förvaltare, byggbolag, andra leverantörer och samarbetspartners, och andra.

▶ PERSONUPPGIFTSBEHANDLING
Varje åtgärd som, helt eller delvis automatiserat, vidtas med personuppgifter, exempelvis att samla in och på olika sätt använda uppgifterna eller lämna ut dem till utomstående. ”Behandling” kan även avse passiva åtgärder som exempelvis lagring av personuppgifter i IT-system.

▶ PERSONUPPGIFTSANSVARIG
Den som bestämmer ändamålen och medlen för en personuppgiftsbehandling och därmed är ansvarig för att behandlingen sker i enlighet med GDPR. Det är typiskt sett ett företag eller en organisation, inte en fysisk person, som avses. Alla behandlingar som en anställd gör i sitt arbete är arbetsgivaren personuppgiftsansvarig för.

▶ PERSONUPPGIFTSBITRÄDE
Ett företag eller organisation som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige och för dennes räkning, exempelvis en tjänsteleverantör som inom ramen för sin leverans får tillgång till personuppgifter.

▶ KÄNSLIGA/SÄRSKILDA KATEGORIER AV PERSONUPPGIFTER
Personuppgifter som exempelvis avslöjar ras eller etniskt ursprung, medlemskap i fackförening eller uppgifter om hälsa. En uppgift om att någon behöver ett handikappanpassat boende är ett exempel på en känslig uppgift.

VAD FÖRÄNDRADES NÄR GDPR ERSATTE PUL?

De flesta av de grundläggande begrepp och regler som gällde enligt personuppgiftslagen (”PUL”) motsvaras av i stort sett samma bestämmelser i GDPR.

Det finns dock vissa områden där GDPR medförde förändringar och då främst i form av ökade krav. Här följer några exempel:

- De krav som måste vara uppfyllda för att ett giltigt samtycke till en personuppgiftsbehandling från en individ ska anses ha lämnats av individen har stärks. Det är därmed inte säkert att ett samtycke som inhämtats för behandling av personuppgifter, som var giltigt under PUL, även är giltigt under GDPR.
- Individens rättigheter har vidare utökats och förstärkts genom GDPR, exempelvis ställs det högre krav på att den information som en personuppgiftsansvarig ska tillhandahålla en individ, vars personuppgifter behandlas, är transparent och tydlig.
- Kraven på informationssäkerhet vid behandling av personuppgifter har ökat genom ett antal nya krav i GDPR. Vid en så kallad personuppgiftsincident, då personuppgifter oavsiktligt sprids eller förstörs, är den personuppgiftsansvarige i vissa fall skyldig att anmäla detta till tillsynsmyndigheten och till individer vars uppgifter incidenten berör.
- Den så kallade missbruksregeln som gällde enligt PUL, och som innebar att behandlingar av personuppgifter i ostrukturerad form (exempelvis i löpande text) inte behövde uppfylla samtliga regler i PUL utan endast kraven att individens personliga integritet inte ska kränkas och att uppgifterna ska skyddas, har försvunnit genom införandet av GDPR. Detta innebär att alla behandlingar, även ostrukturerade behandlingar, styrs av samtliga regler i GDPR.
- Den mest omtalade förändringen i GDPR är de hårda sanktioner som införts för brott mot GDPR, som ökar riskerna med att inte efterleva reglerna.

Fastighetsägarna har nedan sammanställt en lista över de huvudsakliga kraven i GDPR och förslag på åtgärder för att efterleva dem, och därigenom förbättra integritetsskyddet och minska riskerna i din organisations behandling av personuppgifter.

TIO FÖRSLAG TILL ÅTGÄRDER FÖR FÖRBÄTTRAD REGEL-EFTERLEVNAD

Att skapa en överblick, och dokumentera hur din organisation behandlar personuppgifter, är en viktig förutsättning för att kunna verifiera att de krav som följer av GDPR efterlevs. Vi föreslår därför att du börjar ditt arbete med att inventera och dokumentera vilka slags personuppgifter som behandlas, för vilka grupper av individer, samt för vilka olika ändamål dessa behandlingar sker.

Inventeringen förenklas genom att du delar upp din organisations verksamheter i lämpliga delar, för att du ska kunna inventera de olika personuppgiftsbehandlingar som sker inom varje del. Ett exempel på en sådan uppdelning kan vara: HR/ekonomi/admin, kundservice/felanmälan, hyra, bygg/reparation, förvaltning, digitala tjänster/sociala medier.

Ett annat exempel på uppdelning är att utgå ifrån de olika IT-system och externa IT-tjänster som används i organisationens behandling av personuppgifter.

En väl genomförd inventering är till stor hjälp vid din genomgång av de krav och åtgärdsförslag som anges i punkterna nedan, vilken med fördel kan ske utifrån samma indelning av verksamheten/personuppgiftsbehandlingar som inventeringen. Ett sätt att dokumentera arbetet är att upprätta register (se punkt 1 nedan).

1. SE ÖVER OM DET BÖR FÖRAS REGISTER OCH/ELLER UTSES ETT DATASKYDDSOMBUD

▶ *Beskrivning av krav:*

GDPR uppställer ett krav på att personuppgiftsansvariga och personuppgiftsbiträden ska föra register över de behandlingar som genomförs. Ett register ska bland annat ange kategorier av registrerade individer, vilka personuppgifter som behandlas och mottagare till vilka personuppgifterna har lämnats eller ska lämnas

ut. Organisationer som sysselsätter färre än 250 personer är som huvudregel undantagna från detta krav (se GDPR artikel 30). Undantag finns dock, exempelvis om företaget behandlar känsliga personuppgifter.

GDPR anger vidare att en personuppgiftsansvarig och ett personuppgiftsbiträde, i vissa fall, ska utse ett dataskyddsombud som bland annat ska informera, ge råd och övervaka efterlevnaden av GDPR i organisationen (artikel 37–39).

Förslag till åtgärd:
Alla medlemmar bör kontrollera om man omfattas av kravet på att föra förteckning eller inte. Även om huvudregeln säger att organisationer med färre än 250 anställda inte omfattas, anges att de organisationer som behandlar exempelvis känsliga personuppgifter, gör det.

Många bostadshyresvärdar behandlar uppgifter om exempelvis bostadsanpassning, vilket är en känslig personuppgift, och omfattas därmed av kravet. Som nämnts ovan, kan det dessutom vara en god idé att upprätta register för att skapa överblick över organisationens personuppgiftsbehandling och för att kontrollera och dokumentera efterlevnad av GDPR.

2. SÄKRA ATT DE GRUNDLÄGGANDE KRAVEN FÖR BEHANDLING AV PERSONUPPGIFTER FÖLJS

Beskrivning av krav:
GDPR anger ett antal krav som all personuppgiftsbehandling måste uppfylla, bland annat att behandlingen ska vara laglig, korrekt och öppen mot individen, att personuppgifter endast får behandlas för på förhand bestämda och berättigade ändamål, att inte flera uppgifter får samlas in och behandlas än vad som är berättigat för att uppfylla ändamålen, att uppgifterna inte får lagras längre än vad som krävs för att uppfylla ändamålen, att skäliga åtgärder vidtas för att rätta och utplåna felaktiga uppgifter samt att behandlingen av personuppgifter måste ske med lämplig säkerhet (artikel 5).

Förslag till åtgärd:
Se till att din organisation är medveten om och följer de grundläggande kraven vid samtliga behandlingar av personuppgifter.

Kontrollfrågor att ställa kan vara: Behandlar vi dessa personuppgifter endast för de (berättigade) ändamål som de samlades in för? Lagrar eller behandlar vi endast de personuppgifter som behövs för ändamålen? Kontrollerar vi att personuppgifterna är korrekta och uppdaterade (hur ofta uppdaterar vi till exempel våra register över hyresgästers uppgifter)? Raderar (gallrar) vi uppgifterna när de inte längre behövs? Se Fastighetsägarnas och SABOs vägledningar för råd rörande lämpliga gallringsintervaller.

Ett sätt att införa rutiner för uppfyllande av de grundläggande kraven kan vara att ta fram skriftliga policys och instruktioner som beskriver kraven och ger exempel på kontrollfrågor som kan användas i hanteringen av personuppgifter.

3. HA EN RUTIN FÖR HUR, NÄR OCH VAR ARBETE MED PERSONUPPGIFTSBEHANDLING DOKUMENTERAS

Beskrivning av krav:
Enligt GDPR måste den personuppgiftsansvarige kunna visa att de grundläggande kraven ovan faktiskt efterlevs. GDPR kallar detta beviskrav för principen om ansvarsskyldighet (se artikel 5).

Förutom den generella principen om ansvarsskyldighet, anges på flera ställen i GDPR att den som behandlar personuppgifter ska kunna visa att reglerna följs.

Förslag till åtgärd:
Säkerställ att det finns rutiner för hur och var din organisations arbete med GDPR-regelefterlevnad ska dokumenteras, till exempel om och i så fall var register finns (se punkt 1).

Liksom sådana policys och instruktioner som eventuellt tas fram i organisationen för personuppgiftsbehandlingar, gallring, etcetera så bör också rutinerna för dokumentering finnas lätt tillgängliga, exempelvis på intranät.

4. VERIFIERA ATT DET FINNS LAGLIG GRUND FÖR ERA BEHANDLINGAR

Beskrivning av krav:
För att en personuppgiftsbehandling, det vill säga varje enskild åtgärd som vidtas med personuppgifter, ska vara tillåten krävs att den sker med stöd av en av de lagliga grunder som framgår av GDPR.

Exempel på en laglig grund är att det finns ett samtycke från individen, att behandlingen är nödvändig för att fullgöra ett avtal (exempelvis ett hyresavtal eller ett anställningsavtal), att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse (exempelvis driva in

en hyresfordran eller lämna ut uppgifter i en pågående förundersökning om brott), eller att det finns ett berättigat intresse för den personuppgiftsansvarige att behandla uppgifterna som väger tyngre än individens behov av skydd för sin integritet (se artikel 6).

Förslag till åtgärd:
Tillse att det finns laglig grund för alla de behandlingar av personuppgifter som sker i organisationen. Fastighetsägarnas medlemmar kommer i stor omfattning kunna behandla hyresgästens personuppgifter utifrån den lagliga grunden att behandlingen är nödvändig för att fullgöra ett avtal, det vill säga det hyresavtal som finns med hyresgästen.

5. SÄKRA ATT INFORMATIONSSKYLDIGHET OCH ANDRA RÄTTIGHETER FÖR INDIVIDEN UPPFYLLS

Beskrivning av krav:
Individers rättigheter i GDPR liknar i stora drag de rättigheter som fanns i PUL. En individ har rätt att få information av den personuppgiftsansvarige avseende den behandling av individens personuppgifter som sker. För hyresvärdar kan information tillhandahållas i exempelvis hyresavtalet med individen eller i en extern personuppgiftspolicy.

I förhållande till anställda kan informationen tillhandahållas i exempelvis anställningsavtalet eller i en intern personuppgiftspolicy (se artikel 12,13,14). Vidare förstärks i GDPR individers möjlighet att begära bland annat information om behandlingar av individens uppgifter (registerutdrag), rättelse, radering och portabilitet (vilket innebär att personuppgifter på individens begäran ska lämnas till en annan part) (se artikel 12–22).

Förslag till åtgärder:
Se över befintliga informationstexter utifrån kraven i GDPR och vid behov uppdatera eller ta fram nya informationstexter. Säkerställ att det finns kunskap och rutiner för att kunna hantera individers begäran om registerutdrag, raderingar etcetera.

Ett register över de behandlingar av personuppgifter som sker (se punkt 1) kan förenkla arbetet med att identifiera efterfrågade personuppgifter.

6. GRANSKA I VILKEN MÅN DIN VERKSAMHET FÖRLITAR SIG PÅ SAMTYCKE SOM LAGLIG GRUND

Beskrivning av krav:
Genom GDPR ställs det högre krav på hur samtycke erhålls än vad som var fallet enligt PUL. För att ett samtycke ska vara giltigt kräver GDPR att samtycket är en frivillig, specifik, informerad och en otvetydig viljeyttring från individen.

I praktiken innebär detta att det kommer ställas högre krav på att individen aktivt ger sitt samtycke, efter att ha fått information om den personuppgiftsbehandling som är aktuell (se punkt 5 ovan), samt att samtycket inte göms bland övriga avtalsvillkor eller samlas med andra samtycken eller godkännande av villkor (se artikel 6, 7, 8, 9).

Förslag till åtgärd:
Identifiera vilka behandlingar av personuppgifter som genomförs i din organisation med stöd av ett befintligt samtycke som laglig grund, hur sådant samtycke inhämtats samt huruvida samtycket är giltigt enligt GDPR (se över de blanketter, godkännande av villkor på nätet etcetera som används).

Om ett befintligt samtycke inte är giltigt enligt GDPR, kan du behöva inhämta ett nytt samtycke, om ingen annan laglig grund för behandlingen är tillämplig (se punkt 4). Säkerställ att det sätt på vilket nya samtycken inhämtas följer kraven i GDPR. Använd klickrutor eller underskrifter så att det blir tydligt att individen aktivt samtycker till den behandling av personuppgifter som informeras om, separerat från till exempel godkännande av hyresvillkor.

7. VAR FÖRSIKTIG MED ATT BEHANDLA SÄRSKILDA KATEGORIER/KÄNSLIGA PERSONUPPGIFTER OCH UPPGIFTER OM LAGÖVERTRÄDELSER

Beskrivning av krav:
Som huvudregel är det inte tillåtet att behandla särskilda kategorier av/känsliga personuppgifter (se artikel 9). Det finns dock undantag till detta förbud, se bland annat Fastighetsägarnas och SABOs vägledningar för vidare information avseende känsliga personuppgifter i hyresrelationer. Att behandla personuppgifter rörande lagöverträdelser, eller misstanke om sådan, är som huvudregel inte heller tillåtet (se artikel 10).

Förslag till åtgärd:
Säkerställ att din organisations behandling av känsliga personuppgifter begränsas när så är möjligt. Om behandling sker, tillse att uppgifterna omgärdas av tillräcklig och adekvat säkerhet. Begränsa åtkomsten till uppgifterna till endast de personer som behöver ha tillgång till dem. Hantering av uppgifter om lagöverträdelser bör i möjligaste mån undvikas.

8. BEDÖM OM INFORMATIONSSÄKERHETEN I DIN ORGANISATION ÄR TILLRÄCKLIG

Beskrivning av krav:
Kraven på informationssäkerhet vid behandling av personuppgifter höjs genom GDPR och blir mer detaljerade. Det uppställs bland annat allmänna säkerhetskrav, krav på inbyggt integritetsskydd/integritet som standard, att det i vissa fall görs konsekvensanalyser och att incidenter som inträffar med personuppgifter i vissa fall ska rapporteras till tillsynsmyndigheten och till individen vars uppgifter incidenten berör. Informationssäkerhetskrav riktas även mot personuppgiftsbiträdet (se artikel 24,25, 32–36).

Förslag till åtgärd:
Se över i vilken omfattning integritetskänsliga personuppgifter behandlas, exempelvis hyresgästers speciella behov. Informationssäkerhet handlar mycket om att ha tillräcklig säkerhet i förhållande till integritetsrisken för individer. Exempel på åtgärder som kan vidtas för att förbättra informationssäkerheten är kryptering, behörighetsbegräsningar samt utbildning för anställda. Informationssäkerhet är också ett område som är viktigt att beakta och fånga upp i kravställningen vid inköp av IT-utrustning och tjänster.

9. KONTROLLERA OM PERSONUPPGIFTER ÖVERFÖRS TILL TREDJE LAND

Beskrivning av krav:
Det är som huvudregel förbjudet att överföra personuppgifter till ett ”tredje land” (ett land utanför EU/EES). Det finns dock undantag till förbudet, exempelvis om ett tredje land anses uppfylla en adekvat skyddsnivå eller om ett dataöverföringsavtal tecknats enlighet EU Kommissionens standardklausuler (se artikel 44–49).

Förslag till åtgärd:
Granska flödet av personuppgifter inom din verksamhet för att se om det sker överföring av personuppgifter till ett tredje land. Exempelvis förekommer det att leverantörer av IT-tjänster använder sig av dotterbolag, underleverantörer eller servrar som är belägna i ett tredje land. Överförs personuppgifter till tredje land bör du säkerställa att överföringen är laglig. På Datainspektionens hemsida, datainspektionen.se, finns mer information.

10. INVENTERA RELATIONERNA MED PERSONUPPGIFTSBITRÄDEN

Beskrivning av krav:
Ett personuppgiftsbiträde får endast behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner. Leverantörer av IT-tjänster är ofta personuppgiftsbiträden och desamma kan gälla för till exempel störningsjoursfirmor.

Om det föreligger ett personuppgiftsbiträdesförhållande, måste ett skriftligt personuppgiftsbiträdesavtal ingås som anger personuppgiftsbiträdets skyldigheter. Förhållandet mellan personuppgiftsbiträde och personuppgiftsansvarig har i viss mån förändrats genom införandet av GDPR. Ett personuppgiftsbiträde kan exempelvis bli ansvarig för felaktiga behandlingar av uppgifter, en bristande informationssäkerhet och om biträdet inte för register när så krävs. GDPR uppställer även fler tvingande bestämmelser, än vad som var fallet enligt PUL, som ett personuppgiftsbiträdesavtal måste innehålla (se artikel 26–29).

Förslag till åtgärd:
Inventera befintliga biträdesrelationer, både då din organisation är personuppgiftsansvarig och anlitar ett personuppgiftsbiträde och då din organisation är personuppgiftsbiträde. Kontrollera att personuppgiftsbiträdesavtal finns och att avtalet uppfyller de utökade kraven i GDPR. Tillse att personuppgiftsbiträdesavtal upprättas när det saknas.

FASTIGHETSÄGARNA

www.fastighetsagarna.se