Plan- og
Landdistriktsstyrelsen

Carsten Niebuhrs Gade 43
1577 København V
www.plst.dk
Telefon 3330 7010
e-mail plst@plst.dk
Sagsnr.
2023 - 6918
Doknr.
202644
Dato.
30.05.24

Retningslinjer for medarbejdernes praktiske håndtering af informationssikkerhed i Plan- og Landdistriktsstyrelsen

Indholdsfortegnelse:

1. Indledning

Retningslinjerne har til formål at beskrive, hvordan medarbejderne i Plan- og Landdistriktsstyrelsen - herefter styrelsen – i praksis skal håndtere informationssikkerhed.

Retningslinjerne har status som intern tjenesteinstruks til alle ansatte, hvilket betyder, at manglende overholdelse kan medføre disciplinære konsekvenser efter de regler, som gælder for dit ansættelsesforhold.

Retningslinjerne tager afsæt i styrelsens informationssikkerhedspolitik.

2. Organisation og tilsyn

Ansvaret for informationssikkerheden er på direktionens vegne placeret hos informationssikkerhedsudvalget, som bl.a. består af underdirektøren for Organisation, chefen for IT i styrelsen, IT medarbejderne og dernæst den enkelte medarbejder.

- Direktionen har det øverste ansvar for informationssikkerheden i styrelsen.
- Informationssikkerhedsudvalget udfører til daglig den praktiske ledelse, planlægning, implementering og overvågning mv. af informationssikkerheden.
- Hver enkelte medarbejder har et individuelt og særligt ansvar for medvirken til at opretholde informationssikkerheden.

3. Adgangsforhold og lokaler

Styrelsen er sikret med adgangskontrol ved alle indgangsdøre. Du skal ved din adgang bruge de opsatte kortlæsere. Skulle du have glemt dit adgangskort, så henvende dig gerne til Direktionssekretariatet og Administration (ls@plst.dk), som på dagen kan være behjælpelig med at udlåne dig et gæstekort.

Man må kun lukke en person ind, som har et gyldigt ærinde i styrelsen og synligt adgangslabel som udleveres af receptionen, eller som kan fremvise gyldigt adgangskort.

Gæster må i udgangspunktet aldrig gå alene rundt i styrelsens lokaler, og du skal så vidt muligt følge dine gæster ind og ud.

Visse af styrelens lokaler er desuden sikrede gennem det interne låsesystem. Relevante medarbejdere kan ved ansættelsen få adgang til styrelsens aflåste lokaler ved udlevering af nøgler. Udlevering af nøgler skal godkendes af chefen for IT, som dernæst registreres af Direktionssekretariatet og Administration. Opbevares der følsomme eller i øvrigt fortrolige personoplysninger i kontoret (se nærmere i afsnit 4.3), skal dette opbevares aflåst.

4. Klassifikation og behandling af informationer

I styrelsen inddeles dokumenter i fire kategorier: offentlig information, intern information, informationer om personer og fortrolig information. Et dokument kan godt tilhøre flere kategorier. Formålet er at sikre en tilstrækkelig beskyttelse af de enkelte informationer. Den medarbejder, der arbejder med en given information, har ansvaret for at vurdere, hvilken kategori informationen tilhører, og dermed omfanget af beskyttelse af informationen. Medarbejderen skal periodisk tage kategoriseringen op til revurdering.

4.1. Offentlige informationer
Offentlige informationer er informationer, som alle kan få adgang til. Det kan for eksempel være informationer tilgængelige på styrelsens eksterne hjemmesider eller andre informationer, som under normale omstændigheder oplyses til alle, der retter henvendelse herom.

Der er ingen særlige krav til behandling eller opbevaring af offentlige informationer. Ligeledes skal der heller ikke tages nogen særlige hensyn ved destruktion af offentlige informationer.

4.2. Interne informationer
Interne informationer er informationer, som indgår i den daglige drift. Det kan for eksempel være visse informationer på styrelsens intranet. Alle medarbejdere må få adgang til interne informationer.

Som udgangspunkt må interne informationer kun anvendes og kommunikeres internt i styrelsen. Informationerne skal behandles med omtanke, men det er ikke nødvendigt at tage særlige hensyn for at sikre informationerne.

4.3. Informationer om personer
Databeskyttelsesforordningen inddeler personoplysninger i to hovedkategorier: almindelige personoplysninger og følsomme personoplysninger. Herudover er oplysninger om strafbare forhold og om personnummeret særligt reguleret. Endelig anvendes i Danmark begrebet fortrolige personoplysninger.[1]

Kun medarbejdere med et arbejdsbetinget behov må tilgå følsomme og i øvrigt fortrolige personoplysninger. Informationerne skal opbevares sikkert, jf. afsnit 3, og kommunikeres således, at de ikke kan komme uvedkommende i hænde.

I styrelsens ESDH-system (F2) beskyttes visse sager med personoplysninger med en sikkerhedsgruppe, som derved begrænser adgangen til visse typer af informationer.

Digital kommunikation af følsomme og i øvrigt fortrolige personoplysninger gennem usikre netværk, herunder internettet, skal altid ske i krypteret form.

Fortrolige og følsomme data kommunikeres kun gennem sikre kanaler som fx Digital Post, krypterede forbindelse – evt. gennem Statens IT filkasse, hvor data kan deles med kode og udløbsdato.

Digital kommunikation gennem interne netværk, f.eks. fra en arbejdsmail til en anden arbejdsmail inden for styrelsens eller mellem Statens It's kunder, anses for sikker e-post, idet informationsudveksling på interne netværk ikke skal krypteres.

Destruktion af følsomme og fortrolige personoplysninger og i øvrigt fortrolige oplysninger skal ske på sikker vis. Informationer i papirformat skal afleveres i de opstil-

---

1

Almindelige personoplysninger – er alle oplysninger, der ikke er kategoriseret som følsomme. Det kan f.eks. være identifikationsoplysninger som navn og adresse, oplysninger om økonomiske forhold, familieforhold, CV, arbejdsområde, kundeforhold eller andre lignende ikke-følsomme oplysninger. Almindelige personoplysninger kan godt samtidig være fortrolige, jf. nedenfor.
Følsomme personoplysninger – er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, fx fingeraftryk, helbredsoplysninger og oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
Fortrolige personoplysninger i øvrigt – er oplysninger, der efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab. Følsomme personoplysninger vil altid være fortrolige, men ikke alle fortrolige personoplysninger er følsomme. Personnummeret er et eksempel på en fortrolig oplysning, der er særskilt reguleret i databeskyttelsesloven. Herudover vil oplysninger om strafbare forhold, økonomiske, sociale eller andre private forhold efter en konkret vurdering kunne være fortrolige.

lede containere til sikkerhedsmakulering i kopi-rummene. Digitale medier, for eksempel USB-nøgler og harddiske, skal afleveres til IT, der sørger for korrekt destruktion.

4.4. Fortrolige informationer i øvrigt
I dette afsnit omtales håndteringen af fortrolige informationer, der ikke omhandler personer.[2]

Fortrolige informationer skal opbevares sikkert og kommunikeres således, at de ikke kan komme uvedkommende i hænde.

Digital kommunikation af fortrolige oplysninger gennem usikre netværk, herunder internettet, skal altid ske i krypteret form. Vejledning om, hvordan man sender sikkert, findes på Inside.

Som omtalt i afsnit 4.3 skal internt digital kommunikation – f.eks. mellem arbejdsmail hos Statens It's kunder - ikke krypteres.

Der gælder også samme regler som i afsnit 4.3 om destruktion af informationer i papirformat via sikkerhedsmakulering, og brugte digitale medier afleveres til styrelsens IT.

4.5. Søgning og tilgang til informationer og sager
Søgning og tilgang til informationer og sager, herunder i ESDH-systemet, må alene ske som følge af et arbejdsbetinget behov og må aldrig ske i privat øjemed.

5. Anvendelse af styrelsens it-systemer
Du skal låse eller slukke pc-arbejdspladsen, når den forlades i længere tid. Du låser den ved at taste Windows tast + L. At efterlade din PC ulåst betyder, at alle får adgang til dine data. En PC anses som værende forladt, når du har sikret dig, at andre ikke kan tilgå den.

Programmer, der kan hentes fra Statens It's softwarecenter, er forhåndsgodkendt til installation på styrelsens PC'er. Det er ikke tilladt at installere øvrige programmer, men såfremt du måtte have et behov herfor så kontakt gerne IT PLST.

For anvendelse af AI henvises til særskilte retningslinjer.

Når du udskriver dokumenter, skal du opholde dig ved printeren, så uvedkommende ikke får adgang til følsomme eller fortrolige personoplysninger eller fortrolige udskrifter i øvrigt.

6. Passwords
Retningslinjer for passwords varierer for de enkelte systemer, du skal dog altid søge at vælge et password på mindst 12 karakterer med en kombination af store og små bogstaver, tal og specialtegn.

Passwords, som benyttes i arbejdsmæssig sammenhæng, bør ikke anvendes til private formål, og du skal sørge for, at de ikke kommer andre i hænde.

[2] Fortrolige informationer defineres i forvaltningslovens afsnit vedr. tavshedspligt (§ 27 og 28, jf. lov nr. 571 af 19. dec. 1985), samt straffelovens § 152, stk. 3, jf. lovbekendtgørelse nr. 1034 af 29. oktober 2009. Dette inkluderer informationer, som er nødvendige at hemmeligholde af hensyn til det offentliges interesser, herunder udførelsen af det offentliges forretningsvirksomhed. I henhold til forvaltningsloven må den, der virker inden for den offentlige forvaltning, ikke i den forbindelse skaffe sig fortrolige oplysninger, som ikke er af betydning for udførelsen af den pågældendes opgaver. Der gælder desuden tavshedspligt for fortrolige informationer. Fortrolige informationer må således kun behandles af og kommunikeres til personer med et arbejdsmæssigt behov.

Ved din ansættelse udleveres der et midlertidigt password, som du skal ændre ved første log-on.

Genåbning ved spærret konto foretages via Statens It's serviceportal eller service-desk.

7. Lokal- og fællesdrev
SIA-PC'en har et lokalt drev (C-drevet), der kan slettes uden varsel i forbindelse med systemopdateringer og installation af nye programmer mv. dog ikke uden forudgående advisering til bruger eller IT PLST. For at sikre at der altid er backup af data, er det derfor vigtigt, at du arbejder og gemmer data på netværksdrev, F2 eller et af styrelsens øvrige systemer.

Der foretages daglig sikkerhedskopiering af fællesdrev (F: og O: drev) og dit personlige fildrev (H: drevet). Der må kun i begrænset omfang lagres dokumenter uden arbejdsmæssig relevans på drevene.

Fællesdrev er beregnet til medarbejdere i afgrænsede grupper, områder og potentielt hele styrelsen har adgang til drevet og foldere.

Personligt-drev (navnet afhænger af opsætningen) er et drev til lagring af dokumenter, som kun du har adgang til.

Alle filer og informationer, der befinder sig på udstyr udleveret af styrelsen, betragtes fortsat som styrelsens ejendom. Styrelsen har således adgang til alle data – også på personligt-drev – hvis der er en saglig grund herfor.

Personoplysninger, der er sagsdannende, skal håndteres i de relevante fagsystemer, som Statens HR eller F2. Styrelsens fagsystemer tager højde for de gældende lovkrav og regler for databeskyttelse og er derfor et sikkert sted at opbevare personoplysninger. Det er muligt at opbevare personoplysninger i mapper på styrelsens netværksdrev eller i dit Outlook i op til 30 dage. Herefter skal de slettes eller flyttes til et godkendt fagsystem. Du skal tage stilling til adgangsbegrænsningen i F2 eller på det drev og den mappe, filerne placeres i på netværksdrevet. Bestil evt. en lukket mappe hos IT afdelingen.

Personoplysninger, der ikke er sagsdannende, skal slettes, når der ikke længere er et sagligt grundlag for opbevaring af dem. Følsomme og fortrolige personoplysninger skal slettes inden for 30 dage.

Områderne skal periodisk foretage en gennemgang af lokal- og netværksdrevene med henblik på at rydde op i lagrede data. Krypteret data kan ligge ubegrænset på fildrevene uanset deres indhold.

8. Bærbare datamedie
Bærbare medier - bl.a. USB-drev, harddiske og bærbare PC'er - har en væsentlig risiko for at blive tabt, stjålet eller glemt. Beskyt derfor filer på USB-drev mv. med kryptering og hold kodeordet hemmeligt. Din SIA-PC fra Statens It er allerede krypteret.

Du må kun benytte USB-drev mv., der kommer fra en kilde, du har tillid til.

Du kan få hjælp af IT PLST til at kryptere bærbare medier.

Alle medier, som ikke længere skal anvendes, skal afleveres til styrelsens IT med henblik på sikker destruktion.

9. Windows opdateringer og antivirus mv.
Statens It udsender løbende vigtige sikkerhedsopdateringer, og det er nødvendigt at genstarte pc'en for at fuldføre installationerne. Ved arbejdstidens ophør skal man derfor altid logge sig af samtlige systemer og slukke sin PC, så systemopdateringerne gennemføres.

10. Internet
Du skal udvise forsigtighed i forhold til, hvilke websites der besøges, og hvilke informationer du oplyser, såfremt du gør det fra din arbejds- pc, -mobil, -tablet m.m. Din anvendelse af internettet må ikke skade styrelsens omdømme.

Styrelsen tillader privat brug af internettet, forudsat at dette ikke leder til misbrug, sikkerhedskompromittering, påvirker styrelsens omdømme, er uforeneligt med arbejdet i styrelsen eller går ud over den enkeltes arbejdsindsats, samt i øvrigt ligger inden for de fastsatte retningslinjer.

Dokumenter eller andre filer, der hentes eller åbnes direkte fra internettet, skal behandles med stor forsigtighed – specielt hvis afsenderen er ukendt, eller indholdet er usædvanligt.

11. E-mail
E-mail-systemet er som udgangspunkt alene beregnet til arbejdsmæssig brug. Al indgående og udgående e-post tilhører derfor styrelsen. E-post dækker både e-mail, digital Post mv.

Styrelsen tillader dog privat brug af e-mail-systemet, forudsat at dette ikke leder til misbrug, sikkerhedskompromittering, påvirker styrelsens omdømme, er uforeneligt med arbejdet i styrelsen eller går ud over den enkeltes arbejdsindsats, samt i øvrigt ligger inden for de fastsatte retningslinjer.

Det anbefales at mærke privat udgående e-post "privat" i emnefeltet samt at oprette en mappe kaldet "privat" til opbevaring af modtaget privat e-post.

Generelt forudsættes det, at medarbejderne ved al kommunikation opretholder en professionel tone og sprogbrug, form og indhold.

Der må kun sendes e-post, som indeholder følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt til modtagere uden for ministeriet, hvis der benyttes kryptering.

E-post, som indeholder følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt, skal desuden slettes fra e-post-systemet, når de ikke længere er nødvendige og senest efter 30 dage. Oplysninger, der er sagsdannende, skal forinden journaliseres i styrelsens sagsbehandlersystem. Dette gælder både for modtaget og afsendt e-post.

Links, dokumenter eller andre filer, der modtages med e-post, skal behandles med stor forsigtighed – specielt hvis afsenderen er ukendt, eller indholdet er usædvanligt.

12. Hjemmearbejdspladser

Styrelsen stiller hjemmearbejdspladser til rådighed for medarbejderne. Disse løsninger og anvendelsen heraf er også omfattet af alle dele af retningslinjerne for informationssikkerhed.

Når der arbejdes uden for arbejdspladsen, skal man i øvrigt sikre, at uvedkommende ikke kan få adgang til eventuelle papirudskrifter, og at udskifter mv. opbevares sikkert og makuleres på behørig vis – f.eks. ved at medbringe materialet til sikkerhedsmakulering i styrelsen.

Ved arbejde i det offentlige rum skal der tages de nødvendige forholdsregler for at sikre, at følsomme og fortrolige personoplysninger og fortrolige informationer i øvrigt ikke kommer uvedkommende til kendskab. Et skærmfilter kan bestilles hos styrelsens IT.

12.1. Fjernadgang til it-systemerne

Det er muligt at få fjernadgang til styrelsens it-systemer gennem en VPN-opkobling af din SIA PC. Der er ligeledes adgang til Citrix-baserede løsninger. Adgangene styres med to-faktor autentifikation – f.eks. koder modtaget via SMS eller apps – og udstyr til understøttelse af disse elementer af løsningerne er personlige og må ikke videregives eller udlånes.

Citrix-løsningen har af sikkerhedshensyn begrænsninger på overførsel af filer.

Ved brug af fjernadgangene er det vigtigt, at man husker at logge af netværket, når adgangen ikke længere skal benyttes.

Man må ikke benytte offentligt tilgængelige computere – eksempelvis i en lufthavn eller på et bibliotek – til at få adgang til styrelsens systemer.

Der må på intet tidspunkt opbevares arbejdsrelaterede følsomme eller fortrolige personoplysninger eller fortrolige informationer i øvrigt på private pc'er.

Der gøres desuden opmærksom på, at der som led i den generelle systemovervågning, jf. pkt.14, også ved hjemmearbejde foretages registrering af den enkeltes log on, log off og tidsforbrug mv.

12.2. Anvendelse og genudlån af styrelsens pc'er

For pc'er og andet udstyr, som ejes af styrelsen, gælder en række særlige forhold.

Udstyret er alene udlånt i tjenstligt øjemed. Det betyder, at det kun må benyttes af brugeren – udstyret må derfor ikke genudlånes til eksempelvis familiemedlemmer.

Det er brugerens ansvar at sikre, at uvedkommende ikke kan få adgang til data fra eller via pc'en. Bærbare pc'er bør derfor ikke efterlades uovervåget i det offentlige rum og skal så vidt muligt opbevares aflåst. Under rejser skal bærbare pc'er altid medbringes som håndbagage.

13. Anvendelse af mobile enheder

Styrelsen udleverer mobile enheder (mobiltelefoner og iPads) til medarbejderne, som på forhånd er registreret hos Statens It og installeret med Statens It's mobile it

arbejdsplads (MIA), som giver sikker adgang til bl.a. mails og F2 (VMWare One Workspace).

Styrelsen kan uden varsel låse og slette alle data på enheden, hvis den f.eks. tabes, stjæles eller bortkommer, eller sikkerhedskopiere telefonens indhold, hvis den f.eks. skal indgå i en kommissionsundersøgelse.

Medarbejderen skal sørge for, at enheden altid er sikkerhedsopdateret til seneste version.

Den mobile enhed skal være beskyttet af adgangskode eller fingeraftryk. Opstår der mistanke om, at uvedkommende har fået kendskab til koden, skal denne straks skiftes på alle relevante enheder.

Arbejdsrelaterede SMS-beskeder og beskeder på andre beskedtjenester, f.eks. Messenger og Whatsapp, må ikke slettes på mobile enheder, medmindre de udelukkende har et personalerelateret indhold, eksempelvis en SMS-besked om, at man holder fri, beskeder til og fra en tillidsrepræsentant (i kraft af dennes funktion) eller beskeder mellem medarbejder og chef om rent personlige forhold, f.eks. en sygemelding.

Ved leders ophør eller udskiftning af mobilt udstyr skal der tages backup af enheden. Dette sørger IT for og gemmer data efter gældende regler hos Statens It.

13.1 Private enheders adgang til data
En privat enhed kan anvendes til at tilgå bl.a. mails og F2. Dette forudsætter installation af MIA, og medarbejderen accepterer herved, at styrelsen uden varsel kan låse og slette alle data på enheden, hvis den f.eks. tabes, stjæles eller bortkommer, eller sikkerhedskopiere telefonens indhold, hvis den f.eks. skal indgå i en kommissionsundersøgelse.

Enheden skal i øvrigt behandles på linje med en af styrelsen udleveret enhed.
De data, der synkroniseres til private enheder, er forretningsdata. Derfor må mobile enheder, hvortil der er etableret synkronisering til arbejdsmail mv., ikke anvendes af eller udlånes til andre, jf. afsnit 12.2.

Medarbejderen bærer selv eventuelle omkostninger til datatransmission på private enheder, herunder ved rejser til udlandet.

I udgangspunktet ydes der fra styrelsens side *ikke* support til private enheder - herunder opsætning af synkronisering mv.

13.2 Tjenesterejser og private rejser med udstyr, der synkroniserer med F2 og mail
Ved tjeneste- eller privatrejser til udsatte lande uden for EU, som indebærer en større sikkerhedsrisiko pga. terror, uroligheder, krig e.a., skal styrelsens IT-support kontaktes med henblik på vejledning om IT-sikkerhedsmæssige forhold, hvis der medbringes og anvendes enheder, udleveret af arbejdspladsen, eller som tilgår eller synkroniserer med F2, mail mv.

14. Rapportering af hændelser

Hvis en medarbejder har mistanke om eller kan konstatere trusler mod eller brud på informationssikkerheden, skal dette straks rapporteres til styrelsens IT på IT@plst.dk, som inddrager øvrige relevante parter. [3]

Uden for normal arbejdstid kan trusler mod eller brud på informationssikkerheden også rapporteres til Statens It's servicedesk.

Ved rapportering af en hændelse er det vigtigt, at medarbejderen har noteret sig så mange detaljer som muligt. Det er samtidig vigtigt, at medarbejderen ikke selv forsøger at afhjælpe eller undersøge sagen, da problemet uforsætligt kan forværres, ligesom eventuelt bevismateriale kan mistes. Hvis hændelsen er opstået i forbindelse med brugen af en pc, skal medarbejderen sørge for, at skaderne mod netværket søges begrænset – f.eks. ved at slukke pc'en.

Truslerne rettet mod it-brugerne er under stadig forandring, og du kan finde information om de aktuelle trusler på Inside.

For indrapportering af hændelser henvises til særskilte retningslinjer.

15. Sikkerhedskopiering

Relevante data sikkerhedskopieres af IT for at kunne genskabe tabte data. Relevante data er eksempelvis e-mails, data på netværksdrev og data i F2. Genskabelse af den seneste version af et dokument, der er taget backup af, kan ske ved henvendelse til Statens It eller styrelsens IT.

16. Overvågning af it-systemer

Af hensyn til styrelsens driftsstabilitet og sikkerhed foretages jævnlig overvågning af netværket og driftsmiljøet af både Statens It samt Center for Cybersikkerhed, m.fl. uden forudgående varsel.

Styrelsen kan få adgang til din e-post øjeblikkeligt ved mistanke om igangværende misbrug, hacker-angreb, sikkerhedstrusler, efterforskning, reetablering efter sikkerhedshændelser eller genopretning efter nedbrud.

Derudover kan din nærmeste chef eller formanden for informationssikkerhedsudvalget beslutte, at der skal gives adgang til din e-post. Det kan f.eks. være, hvis du er utilgængelig i en længere periode, eller din ansættelse er ophørt. Privat e-post i mailsystemet, som ikke har nogen relation til styrelsen, læses som udgangspunkt ikke af andre.

Af hensyn til styrelsens drifts- og informationssikkerhed foretages løbende sikkerhedskopiering af log-filerne. Sikkerhedskopien opbevares i to år.

---

[3] Sikkerhedsbrud, fejl eller sårbarheder inkluderer:

- Tab af it-udstyr, mobiltelefon, fysiske dokumenter mv.
- Hvis der er adgang til informationer, som ikke burde være tilgængelige.
- Hvis adgang til informationer, som burde være tilgængelige, er mistet.
- Hvis informationer kan være kommet de forkerte personer i hænde.
- Hvis retningslinjer eller procedurer ikke følges.
- Fejl i systemer eller udstyr.
- Angreb fra virus, skadelige programmer eller lignende i it-systemerne.
- Enhver anden hændelse, der vedrører fortroligheden, integriteten eller tilgængeligheden af styrelsens informationer.

17. Systemspecifikke retningslinjer og vejledninger

For flere af styrelsens systemer, f.eks. F2 og Navision, gælder specifikke sikkerhedsinstrukser og vejledninger. Brugerne vil blive bekendtgjort med disse i forbindelse med oprettelse som bruger af systemet.

18. Oplysningspligt over for borgerne

Af nedenstående følger nærmere beskrivelse af, hvordan du som medarbejder i styrelsen skal håndtere oplysningspligten over for borgerne.

18.1. GDPR helt kort

GDPR står for General Data Protection Regulation, som er EU-lovgivning fra 2018. Lovgivningen kaldes også Persondataforordningen eller Databeskyttelsesforordningen og handler om at beskytte borgernes personoplysninger. En del af lovgivningen handler om, at Plan- og Landdistriktsstyrelsen - som såkaldt dataansvarlig myndighed - har oplysningspligt ift. borgerne.

"Personoplysninger" er enhver form for information, som kan henføres til en identificeret eller en identificerbar fysisk person.

Det gælder oplysninger om f.eks.:

1. Navn, adresse mv. (kaldet almindelige personoplysninger)
2. Personers politiske orientering, fingeraftryk mv. (kaldet særlige personoplysninger)
3. Personer, som er i kontakt med styrelsen som følge af deres profession, f.eks. journalister, folketingsmedlemmer, medarbejdere i andre ministerier, advokater mv.,
4. Såkaldte bipersoner, dvs. personer som ikke er genstand for sagsbehandling i styrelsen, og som ikke selv har henvendt sig til styrelsen.

"Behandling" af personoplysninger omfatter enhver aktivitet i forhold til persondata, f.eks. indsamling, registrering, organisering mv. Det gælder uanset om behandlingen er foretaget digitalt eller ikke-digitalt.

I praksis betyder denne brede definition for Plan- og Landdistriktsstyrelsen, at stor set al virksomhed i styrelsen omfatter en behandling af personoplysninger.

18.2. Hvad betyder oplysningspligten?

GDPR-lovgivningen indeholder en række rettigheder for borgeren. En af disse rettigheder indebærer, at vi som dataansvarlig myndighed har pligt til af egen drift at give den borger, personoplysninger vedrører, nogle bestemte informationer (oplysningspligten).

Oplysningspligten gælder som udgangspunkt uanset, om vi har indhentet eller modtaget personoplysninger fra den registrerede selv, eller om vi har indhentet eller modtaget oplysninger fra andre end den registrerede. Formålet med pligten er at skabe gennemsigtighed, så den registrerede kan varetage sine interesser.

Det betyder, at vi som medarbejdere i en række situationer skal orientere borgeren om, at vi har modtaget og/eller behandlet personoplysninger om borgeren.

18.3. Hvordan overholder vi oplysningspligten?

Der skelnes mellem, om vi har modtaget/indhentet personoplysningerne fra borgeren selv eller fra andre.

Hvis vi har indhentet/modtaget oplysninger fra borgeren selv, skal vi i styrelsen orientere borgeren selv om, hvordan vi håndtere personoplysninger. Det gør vi ved, at:
1. Have nærværende beskrivelse for håndtering af personoplysninger
2. Alle medarbejders signatur indeholder et link til personoplysningsafsnittet på PLST.dk.

Hvis vi har indhentet/modtaget oplysninger fra andre end den registrerede selv, kan vi normalt ikke regne med, at den registrerede er bekendt med, at vi har modtaget oplysningerne, og hvordan vi behandler dem. Derfor skal vi i styrelsen – for at overholde informationspligten – orientere borgeren om, at vi har indhentet/modtaget oplysninger fra andre.

Eksempler:
- En borger klager over en medarbejder i Plan- og Landdistriktsstyrelsen. Vi skal orientere den pågældende medarbejder om, at vi behandler personoplysninger om vedkommende og give en række nærmere informationer.
- En borger er utilfreds med Ankestyrelsens udtalelse i en tilsynssag. Vi indhenter akterne i borgerens sag fra Ankestyrelsen for at vurdere, hvordan vi skal behandle sagen. Vi skal orientere borgeren om, at vi har indhentet oplysninger om den pågældende og give en række nærmere informationer.

Konkret skal sagsbehandleren sende en skrivelse til borgeren, hvori der orienteres om, at styrelsen behandler personoplysninger om borgeren.

Der er udarbejdet en skabelon til dette brev, som ligger i F2.

18.4. Spørgsmål fra borgere mv.
Hvis du bliver kontaktet af en borger eller andre, der har modtaget et orienteringsbrev fra styrelsen, og som er i tvivl om, hvordan det skal forstås, eller hvordan han eller hun skal forholde sig, kan du oplyse følgende:
1. Plan- og Landdistriktsstyrelsen modtager og videregiver oplysninger på helt sædvanlig vis og kun i det omfang, det er nødvendigt. Det er ikke noget nyt.
2. Efter persondatareglerne skal den, som oplysningerne vedrører, orienteres om det for at sikre åbenhed om behandlingen af personoplysninger. Det er netop hensigten med vores orienteringsbrev
3. Du kan også henvise vedkommende til at kontakte styrelsens databeskyttelsesrådgiver.

18.5. Hvornår skal vi give informationen (tidsfrister)?
Orienteringen bør gives så tidligt som muligt og normalt inden for 10 dage efter modtagelsen af personoplysningerne.

Hvis personoplysningerne stammer fra andre end den registrerede, og du ved, at du i løbet af kort tid skal kommunikere med den registrerede, må du godt vente med at opfylde oplysningspligten til du alligevel skriver til vedkommende.

Hvis personoplysningerne stammer fra andre end den registrerede, og de er bestemt til at blive videregivet til en anden modtager, må du ligeledes godt vente med at opfylde oplysningspligten til du videregiver oplysningerne første gang.

I begge ovenstående tilfælde må der dog højst gå en måned efter, at du har indsamlet eller modtaget oplysningerne.

18.6. Undtagelser fra oplysningspligten
Oplysningspligten gælder ikke, hvis den registrerede allerede er bekendt med de oplysninger, Plan- og Landdistriktsstyrelsen skal give. Hvis du kan godtgøre, at det er tilfældet i den konkrete sag, kan du undlade at sende en persondataorientering.

Efter databeskyttelseslovens § 22 kan du også undlade at iagttage din oplysningspligt, hvis den registreredes interesse i at få kendskab til oplysningerne må vige for:
1. Afgørende hensyn til enten private interesser, herunder hensynet til den pågældende selv, eller
2. Afgørende hensyn til offentlige interesser, herunder afgørende hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed og forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger.

Hvis oplysningerne er indsamlet eller modtaget fra andre end den registrerede, gælder endvidere følgende undtagelser:
1. Hvis det viser sig umuligt, f.eks. hvor du har modtaget oplysninger om en person med et meget almindeligt navn, men ingen andre oplysninger, der kan hjælpe dig med entydigt at identificere, hvem det er.
2. Hvis det vil kræve en uforholdsmæssig stor indsats, navnlig hvor behandlingen sker til videnskabelige eller statistiske formål.
3. Hvis orienteringen vil gøre det umuligt eller i alvorlig grad hindre opfyldelse af formålene med behandlingen at give oplysningerne.
4. Hvis styrelsen udtrykkeligt ved lov er blevet pålagt at indsamle eller videregive personoplysningerne.
5. Personoplysningerne skal forblive fortrolige som følge af særlige tavshedspligtsbestemmelser.

Håndtering af såkaldte bipersoner:
Plan- og Landdistriktsstyrelsen vil normalt ikke selv indhente oplysninger om såkaldte bipersoner, dvs. personer som ikke er genstand for nogen sagsbehandling, og som ikke selv har henvendt sig til styrelsen. Styrelsen modtager imidlertid somme tider den type oplysninger uopfordret, f.eks. ved at en klager omtaler en anden person i en e-mail.

Du vil i disse tilfælde ofte i videre omfang end i forhold til andre registrerede, fortsat kunne anvende undtagelserne til oplysningspligten, da opfyldelse af oplysningspligten her ofte vil være umulig eller kræve en – relativt set i forhold til den beskedne rolle, bipersonen spiller i sagen – uforholdsmæssig stor indsats.

I praksis vil vi i Plan- og Landdistriktsstyrelsen kun sjældent have sager, der er undtaget fra oplysningspligten.

Såfremt du vurderer, at der ikke er behov for at iagttage oplysningspligten, skal du notere denne vurdering på sagen.

19. Ikrafttrædelse
Nærværende retningslinjer træder i kraft den 1. august 2024.