Kom i gang med udarbejdelse af dokumentation

GDPR tjekliste til webshopejere

ScanNet

GDPR - Tjekliste til Webshopejere

- [ ] 1. Få styr på de vigtigste begreber 2
- [ ] 2. Fortegnelse over persondata 3
- [ ] 3. Behandlingsgrundlag 4
- [ ] 4. Privatlivspolitik 5
- [ ] 5. Databehandleraftaler 6
- [ ] 6. Pligt til at slette persondata 7
- [ ] 7. De registreredes rettigheder 8
- [ ] 8. Skriftlig risikovurdering 9
- [ ] 9. Beredskabsplan 10
- [ ] 10. Overførsel til tredjelande 11

Denne tjekliste er vores bud på, hvilken dokumentation der er relevant for dig som webshopejer at udarbejde i forbindelse med Persondataforordningen.

Det er vigtigt at understrege, at denne tjekliste og de tilhørende afsnit for hver kategori skal ses som en hjælp til jer og ikke en facitliste.

Vi kan derfor ikke garantere, at du som webshopejer efterlever reglerne blot ved at benytte denne tjekliste, da der kan gælde særlige omstændigheder for dig og din virksomhed.

Er du i tvivl om noget, anbefaler vi, at du rådfører dig med en advokat.

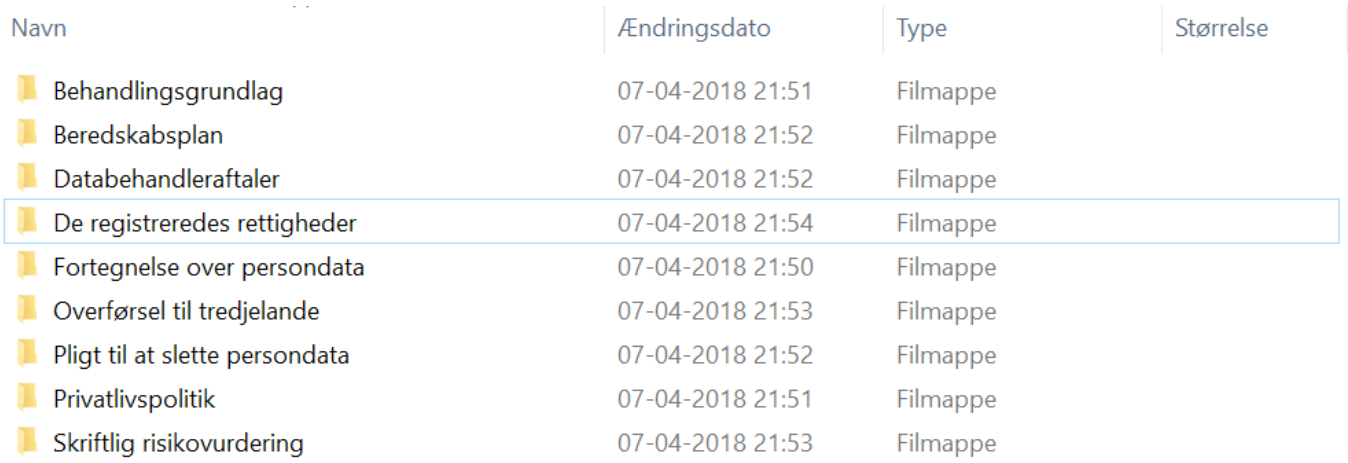
God læselyst!

Indledning

Hensigten med denne tjekliste er at hjælpe dig som webshopejer med at komme i gang med at få udarbejdet en del af den dokumentation, som er nødvendig for at kunne efterleve den nye Persondataforordning (herefter kaldet GDPR).

Det er vores overbevisning, at når du har udarbejdet en fyldestgørende dokumentation i de ovenstående kategorier på tjeklisten, så er du godt på vej.

Et forslag kunne til en start være at oprette en overordnet mappe og kalde den "Virksomhedens dataforhold". Herefter opretter du mapper for hver kategori i tjeklisten, så du har god styring med processen.



Navn	Ændringsdato	Type	Størrelse
Behandlingsgrundlag	07-04-2018 21:51	Filmappe	
Beredskabsplan	07-04-2018 21:52	Filmappe	
Databehandleraftaler	07-04-2018 21:52	Filmappe	
De registreredes rettigheder	07-04-2018 21:54	Filmappe	
Fortegnelse over persondata	07-04-2018 21:50	Filmappe	
Overførsel til tredjelande	07-04-2018 21:53	Filmappe	
Pligt til at slette persondata	07-04-2018 21:52	Filmappe	
Privatlivspolitik	07-04-2018 21:51	Filmappe	
Skriftlig risikovurdering	07-04-2018 21:53	Filmappe	

Når mapperne er oprettet, starter arbejdet med at fylde dem med relevant dokumentation. Hvis det virker uoverskueligt, så tag én ting eller to ad gangen.

Vi har forsøgt at opbygge tjeklisten i prioriteret rækkefølge, så vi anbefaler, at du starter i toppen og arbejder dig ned igennem hvert punkt. Ved at starte med at lave fortegnelsen har du et godt udgangspunkt.

ScanNet

1. Få styr på de vigtigste begreber

Almindelige oplysninger

- Navn
- Adresse
- Telefonnummer
- Fødselsdato
- Oplysninger om uddannelse
- Nuværende stilling
- Oplysninger om løn og økonomiske forhold
- Kundeforhold

Almindelige oplysninger er de personoplysninger, der kan identificere en person, men som ikke falder ind under kategorien "følsomme oplysninger".

Ovenstående liste med almindelige oplysninger er ufuldstændig, dvs. listen indeholder blot eksempler på almindelige oplysninger.

Hovedreglen er stadig, at alle personoplysninger, der kan identificere en person, men som ikke er følsomme personoplysninger, er almindelige personoplysninger.

Følsomme oplysninger

- Oplysninger om race eller etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Helbredsoplysninger
- Oplysninger om seksuelle forhold og orientering
- Oplysninger om strafbare forhold
- Generiske og biometriske data

Listen med **følsomme oplysninger** er fuldstændig, altså indeholder den samtlige kategorier, der findes af følsomme oplysninger.

Dataansvarlig: Personen eller virksomheden, der indsamler data og har ejerskabet over disse data. Den dataansvarlige har ansvaret for, at de indsamlede data behandles ansvarligt, også af leverandører og evt. tredjeparter.

Databehandler: Personen eller virksomheden, der behandler data på vegne af den dataansvarlige. Databehandleren må kun behandle data efter den dataansvarliges instruks.

Datasubjekt: En fysisk person, hvis persondata behandles af en dataansvarlig eller databehandler.

2. Fortegnelse over persondata

Som webshopejer er du dataansvarlig for de persondata, du indhenter om dine kunder i forbindelse med et salg.

Hvis du sender nyhedsbreve til kunden, og du til dette formål indhenter deres navn og e-mailadresse, så er du også dataansvarlig for disse data. Det samme gælder de persondata, du indhenter om dine medarbejdere - det gælder både kontaktoplysninger, CPR-nummer og billeder.

Som dataansvarlig skal du udarbejde en fortegnelse over den dataindsamling og databehandling, du foretager.

Hvorfor? Det er krav efter GDPR, at man har en skriftlig og elektronisk fortegnelse, der kan vise al behandlingsaktivitet, der sker i forhold til persondata i virksomheden.

Det kan virke uoverskueligt, og det er en større proces at få lavet en sådan fortegnelse, så det er med at komme i gang.

Hvordan gør jeg? Du bliver nødt til at undersøge forskellige forhold i virksomheden for at kunne udarbejde fortegnelsen. Hvis du har medarbejdere i virksomheden, kan det blive nødvendigt at interviewe dem, som har viden om virksomhedens databehandling og processer.

Du skal have undersøgt følgende forhold:

- Hvilke kategorier/typer af persondata behandler virksomheden?
- Hvilke behandlinger af persondata virksomheden foretager, og hvad formålet med den enkelte behandlingsaktivitet er?
- Hvem er dataansvarlig og databehandler for den enkelte behandlingsaktivitet?
- Hvilke kategorier af registrerede personer behandler virksomheden persondata om, f.eks. ansatte, kunder, ansøgere eller lign.?
- Hvilke samarbejdspartnere eller andre aktører videregiver virksomheden persondata til?
- Til hvilke tredjelande sker der overførsel af persondata – hvis nogen – og i så fald, hvad er grundlaget for overførsel?
- Hvornår slettes eller vil persondata blive slettet?
- Svarer sikkerhedsniveauet i virksomheden til de risici, der er forbundet med behandlingen af persondataen?

Minimumskrav til indholdet i fortegnelsen for en dataansvarlig virksomhed

1. Navn og kontaktoplysninger på den dataansvarlige virksomhed
2. Formålene med behandlingen
3. Kategorierne af registrerede (personer), personoplysninger og modtagere
4. Tredjelandsoverførsel
5. Forventede tidsfrister for sletning
6. Sikkerhedsforanstaltningerne

Et rigtig godt hjælpeværktøj til at få udarbejdet fortegnelsen findes på følgende hjemmeside, hvor linket til regnearket findes nederst:

Nyt gratis værktøj kan lette arbejdet med persondataforordningen

ScanNet

3. Behandlingsgrundlag

Den dataansvarlige skal vurdere, hvorvidt behandlingen af persondata sker lovligt.

Hvorfor? Fordi man ALTID skal have en lovlig grund til at indsamle og behandle al den persondata, som virksomheden er i besiddelse af eller kommer i besiddelse af.

Hvordan gør jeg? Nedenfor er de fire behandlingsgrundlag nævnt, som vi mener vil være mest relevante for webshopejere. Hvis man behandler almindelige oplysninger, er behandlingen heraf lovlig, hvis:

Behandling af persondata sker for at opfylde en aftale
Hvis du indsamler navn og adresse for at kunne levere et produkt til en kunde, så har du en lovlig grund til at behandle dataene, du indsamler, fordi du skal bruge dataene til at opfylde købsaftalen med kunden.

Behandling af persondata sker efter den registrerede har givet aktivt samtykke hertil
Indsamler du f.eks. en kundes e-mailadresse til at sende nyhedsbreve, eller bruger du en kundes kontaktoplysninger i markedsføringssammenhænge, så skal kunden give særskilt samtykke til denne behandling.
Du skal også indhente samtykke fra en medarbejder, hvis du ønsker at bruge et billede af dem på virksomhedens hjemmeside.
Hvis du vil have gode eksempler på, hvornår samtykke er nødvendigt, så læs Datatilsynets vejledning om samtykke her:
Vejledning om samtykke

Behandling af persondata sker som led i en juridisk forpligtigelse
Enhver behandling, som udføres for at overholde anden lovgivning, betragtes også som lovlig behandling i henhold til GDPR.

Behandling af persondata sker i den dataansvarliges legitime interesse
Hvis behandlingen af persondata er nødvendig for at forfølge den dataansvarliges legitime interesse, er den også tilladt i henhold til GDPR. Et eksempel kunne være at samle og behandle data for at identificere personer ansvarlige for hackerangreb, svig og lign.

Vær opmærksom på, at der findes flere behandlingsgrundlag end de fire nævnte – se dem her og læs mere om, på hvilke grundlag behandling af følsomme oplysninger kan ske:
Grundlag for behandling af personoplysninger

For hver type af persondata virksomheden behandler, så tag stilling til og få dokumenteret, hvilken/hvilke af behandlingsgrundlagene der giver jer ret til at behandle de pågældende persondata.

4. Privatlivspolitik

Når du har lavet din fortegnelse over den persondata, I behandler i virksomheden, er det tid til at få skrevet privatlivspolitikker, som giver kunder og medarbejdere information om, hvilke persondata I indsamler om dem, og hvad I har tænkt jer at gøre med de data.

Hvorfor? Fordi GDPR pålægger alle dataansvarlige en oplysningspligt. Du skal derfor sørge for, at du skriftligt oplyser dine kunder/medarbejdere om, hvad der sker, når de overlader nogle af deres persondata til din virksomhed.

Hvordan gør jeg? Der skal udarbejdes en privatlivspolitik rettet mod kunderne og en privatlivspolitik rettet mod medarbejderne.

Når oplysningerne indhentes fra kunderne/medarbejderne, skal der altid gives følgende oplysninger:

- Identitet og kontaktoplysninger
- Formålene og grundlaget for behandlingen af personoplysninger
- Anvendelse af legitime interesser
- Andre modtagere af personoplysningerne
- Tredjelandsoverførsel

Når oplysningerne indhentes fra kunderne/medarbejderne, skal den dataansvarlige – efter en konkret vurdering - give oplysninger om følgende:

- Tidsrummet for opbevaring af oplysninger
- Den registreredes rettigheder
- Pligt til at meddele personoplysninger

Det vil i de fleste tilfælde være fornuftigt at give oplysninger om alle de nævnte punkter, da du på den måde sikrer gennemsigtighed omkring den databehandling, du foretager. Hvis du behandler persondata på det grundlag, at du som dataansvarlig har en legitim interesse heri, så er det i den sammenhæng, at punktet ”anvendelse af legitime interesser” bliver relevant at nævne i privatlivspolitikken.

Hvis du indsamler persondata om kunder og medarbejdere, som du får fra en tredjepart i stedet for at indsamle dem direkte hos kunden eller medarbejderen, så skal der gives flere oplysninger. Læs mere herom under ”oplysningspligt” på:
Den registreredes rettigheder

5. Databehandleraftaler

Hvis du overlader noget af det persondata, du indsamler, til behandling hos en tredjemand, så skal du indgå en databehandleraftale med den pågældende virksomhed.

Hvorfor? Det skal du, fordi du kun kan behandle persondata ansvarligt, hvis du sørger for, at den tredjemand, du overlader data til, også foretager en sikker behandling heraf. Derfor skal du give tredjemand en skriftlig instruks om rammerne for den databehandling, som skal foretages, og det er det, der er reguleret i en databehandleraftale.

Hvordan gør jeg? Det er endnu ikke afklaret, hvem der har ansvaret for, at der er indgået en databehandleraftale. Men som vi ser det, ligger det primære ansvar for at indgå en databehandleraftale med sine leverandører hos den dataansvarlige. Dog kan man argumentere for, at databehandleren ikke kan behandle data uden instruks, så det derfor er i begge parters interesse, at der foreligger en databehandleraftale.

Mange databehandlere vil dog tilbyde deres egen aftale, og det er helt i orden, at du som dataansvarlig indgår den aftale, som databehandleren tilbyder. Dog skal du være opmærksom på, at følgende ting skal være reguleret på passende vis i aftalen:

- En beskrivelse af emnet, varigheden, arten og formålet med behandlingen, typen af data, kategorier af datasubjekter samt
- den dataansvarliges forpligtelser og rettigheder
- Instruktionsbeføjelse
- Krav om fortrolighed hos autoriserede personer
- Betingelse om, at der kun må bruges underdatabehandlere med den dataansvarliges forudgående skriftlige samtykke
- Betingelse om, at databehandleren bistår med at besvare henvendelse fra datasubjekter
  Krav om implementering af sikkerhedskrav
  Betingelse om, at databehandleren bistår med overholdelse af forpligtelserne ift. personoplysningssikkerhed:
    - Behandlingssikkerhed
    - Anmeldelse af sikkerhedsbrud til myndighed og eventuelt datasubjekter
    - Konsekvensanalyse og forudgående høring
- Betingelse om, at persondata skal slettes eller returneres ved aftalens ophør
- Underretning om ulovlig instruks
- Betingelse om, at databehandleren dokumenterer overholdelse af aftalen og tillader revision og inspektion

Mange af de skabeloner, der findes online, vil være meget omfattende og komplekse, og du bør derfor være meget opmærksom på, hvad der står i de aftaler, du skriver under på.

Hos ScanNet indgår vi en aftale med vores kunder, som både er kortfattet og til at forstå, men som samtidig lever op til kravene i GDPR.

Du kan anmode om at få ScanNets databehandleraftale tilsendt på følgende hjemmeside:
scannet.dk/compliance

ScanNet

6. Pligt til at slette persondata

Som dataansvarlig skal du sørge for at få fastlagt procedurer for sletning af persondata.

Hvorfor? Fordi GDPR kræver, at du skal slette persondata, der ikke længere er nødvendig eller relevant for virksomheden at have liggende.

Generelt har GDPR fokus på dataminimering, hvilket betyder, at du kun bør indsamle lige præcis den data, du reelt har behov for, og når den ikke længere er relevant og nødvendig, så skal du slette den.

Dette nye tiltag har affødt rigtig mange spørgsmål, fordi man tidligere bare har haft alt indsamlet data liggende. Så der er ikke nogen, der førhen har taget stilling til, hvor længe det egentlig er relevant at have persondata opbevaret, eller har opstillet et overblik over, hvilke danske lovgivninger der kræver, at man opbevarer persondata i et vist tidsrum.

Det er desuden vigtigt at forstå, at der i GDPR ikke er angivet nogle præcise tidsfrister for sletning.

Hvordan gør jeg? Det, du er forpligtet til, er at angive i fortegnelsen, hvilke forventede tidsfrister for sletning I har for hver kategori af persondata. Så tag hver kategori af data for sig og tag stilling til, hvor længe I har behov for at gemme det. Skriv jeres overvejelser og argumenter vedrørende jeres "Slettepolitik" ned i et dokument.

I det følgende har vi prøvet at nævne nogle forskellige forhold, som måske kan være relevante for dig som webshopejer. Som nævnt kan vi kun give et bud på, hvad du skal have med i dine overvejelser, når du fastsætter din politik for, hvor længe du vil gemme sine persondata:

> *Har du et aktivt kundeforhold, f.eks. med en kunde som har købt et abonnement eller en form for løbende ydelse, så vil persondata på denne kunde være relevant at have, så længe kundeforholdet står på.*
>
> *Regnskabsmateriale skal opbevares i 5 år, fra udgangen af det regnskabsår materialet vedrører, i henhold til Bogføringsloven.*
>
> *Stiller du en garanti på et produkt i et bestemt tidsrum, så kan det være relevant at have visse data om den kunde, du har givet garantien.*
>
> *Regler i Købeloven giver forbrugerne 2 års reklamationsret.*
>
> *Hvis I behandler persondata på baggrund af et samtykke, og dette samtykke tilbagekaldes, så bør disse persondata slettes.*
>
> *Oplysninger om medarbejdere kan gemmes i fem år (efter medarbejderen forlader arbejdspladsen), da krav, der relaterer sig til ansættelsesforholdet, forældes efter fem år i henhold til Forældelsesloven.*

Hvis det slet ikke er praktisk muligt for dig at fastsætte tidsfrister for sletning, eller det ikke er teknisk muligt at indføre automatisk sletning, så må du sørge for i hvert fald at have beskrevet en procedure for, hvordan I vil sikre jer, at I får taget løbende stilling til, hvilke persondata I skal gemme, og hvilke der skal slettes.

7. Datasubjekternes rettigheder

Den dataansvarlige skal være i stand til at give kunder og medarbejdere indsigt i, hvilke persondata der er registreret om det pågældende datasubjekt, samt at slette disse persondata, hvis det kræves af datasubjektet.

Hvorfor? Fordi datasubjekter nu skal have ret til at vide, præcis hvilke data virksomhederne behandler om dem, og hvad de bruger dem til. Det er derfor vigtigt, at du kender til rettighederne og har en plan for, hvordan du vil efterkomme anmodninger fra kunder.

Hvordan gør jeg? ScanNet vil sørge for, at det i webshoppen er muligt at fremsøge alle persondata, der er registeret om en bestemt kunde i shoppen. Inden du sender oversigten over de persondata, du har registreret, er det vigtigt, at du kigger det hele grundigt igennem, så du ikke sender persondata, som ikke relaterer sig til den pågældende kunde.

ScanNet vil også sørge for, at al data kan slettes både manuelt og automatisk, således at al data registeret om en kunde kan slettes. Men det er meget vigtigt at huske, at du ikke bare skal slette al data, så snart en kunde henvender sig. Du har f.eks. altid ret til at opbevare data, som du er pålagt at opbevare i en periode i henhold til national lovgivning.

Rettighederne, som man skal kunne efterleve, er følgende:

Datasubjektet har ret til at se egne persondata (indsigtsretten)

Datasubjektet har ret til at få slettet persondata om vedkommende selv. Se hvornår datasubjektet har denne ret på følgende hjemmeside: Ret til sletning - hvornår?

Datasubjektet har krav på at få sine oplysninger rettet. Se hvornår datasubjektet har denne ret på følgende hjemmeside: Krav på rettelse - hvornår?

(Retten til at tage sine oplysninger med – dataportabilitet – er mindre relevant for webshopejere og er derfor udeladt her)

Udarbejd en udførlig plan for, hvordan du vil håndtere anmodninger fra kunder. Du kan f.eks. tage stilling til følgende:

Hvem der skal udføre opgaven.

Hvordan du sikrer dig, at kunden rent faktisk har ret til at få oplysningerne udleveret eller slettet. Der skal fastsættes nogle retningslinjer for, hvordan kunden legitimerer sig.

Hav nogle retningslinjer for, hvor hurtigt du skal udføre opgaven. F.eks. skal du fremsende svar på en anmodning om indsigt uden unødig forsinkelse, men senest en måned efter modtagelse af anmodningen.

Fastlæg at der skal ske en endelig screeningsproces, inden du udleverer oplysninger eller sletter oplysninger, så du kan undgå, at der sker fejl.

8. Skriftlig risikovurdering

Når du har fået overblik over, hvilke persondata I behandler, og hvordan det sker, skal du danne dig et overblik over de risici, der er forbundet med jeres behandling af dataene. Der skal altså foretages en risikovurdering.

Hvorfor? Fordi GDPR kræver, at du fastsætter passende tekniske og organisatoriske foranstaltninger for at passe bedst muligt på de persondata, du indsamler. Du er derfor nødt til at foretage en vurdering af, om jeres sikkerhedsforanstaltninger er tilstrækkelige i lyset af de risici, der er forbundet med jeres behandling.

Hvis I alene behandler almindelige oplysninger, stilles der mindre krav til sikkerhedsforanstaltningerne, end hvis I behandler følsomme oplysninger, men vurderingen skal foretages uanset.

Hvordan gør jeg? I risikovurderingen skal du, for de persondata I behandler, vurdere, om der er risiko for:

- Hændelig eller ulovlig tilintetgørelse
- Tab
- Ændring
- Uautoriseret videregivelse

Når du har udarbejdet en risikovurdering, skal du indføre et passende sikkerhedsniveau i jeres virksomhed. Her stiller GDPR krav om både passende tekniske og organisatoriske foranstaltninger.

Tekniske sikkerhedsforanstaltninger er f.eks. brug af passwords ved log-in i et system, antivirus, kryptering af e-mails, logning af behandlingsaktiviteter, herunder tilgang til persondata, men det kan også være videoovervågning af lokaliteterne, logning af personer med adgang til bygningen, hvor persondata kan tilgås mv.

Organisatoriske sikkerhedsforanstaltninger skal indføres generelt i ledelsen og gennemføres ved udarbejdelse af procedurer og retningslinjer til jeres medarbejdere.

Det kan f.eks. betyde uddannelse af medarbejderne i persondatasikkerhed, så de er forberedte på og oplyste om korrekt og sikker behandling af persondata. Derudover kan det være fornuftigt at udarbejde retningslinjer for medarbejdernes behandling af dokumenter og e-mails, der indeholder persondata, og det gælder både i elektronisk og i fysisk form.

Det er faktisk op til jer, hvilke sikkerhedsforanstaltninger I vil implementere i jeres virksomhed, for GDPR opstiller ingen minimumskrav eller konkrete forpligtelser i forhold til, hvilke sikkerhedsforanstaltninger der træffes. Vurderingen af hvad der er nødvendigt, ligger således hos dig.

I den forbindelse er det vigtigt, at du beskriver de overvejelser, du gør dig under processen i et elektronisk dokument, så du har noget dokumentation for, at du har undersøgt omstændighederne og har taget stilling til, hvilke sikkerhedsforanstaltninger der er nødvendige for jeres virksomhed.

9. Beredskabsplan - Hvis der sker et brud på persondatasikkerheden – hvad så?

Et brud på persondatasikkerheden betyder, at der er blevet lækket noget persondata, og så er det nødvendigt at sætte gang i beredskabet. Til det formål skal du have udarbejdet en beredskabsplan.

Hvorfor? Fordi du som dataansvarlig skal underrette Datatilsynet inden for 72 timer, hvis persondata er blevet kompromitteret. Hvis det ikke er persondata, der er blevet lækket, men andre former for data, så skal der ikke ske underretning.

Tidsfristen for underretning på de 72 timer løber fra tidspunktet for opdagelsen af databruddet eller fra det tidspunkt, hvor man bliver underrettet om bruddet fra sin databehandler, så du bliver nødt til at have helt klare og nedskrevne retningslinjer for, hvordan du vil håndtere situationen.

Hvordan gør jeg? Udarbejd en udførlig plan for, hvordan du vil håndtere et brud på persondatasikkerheden. I det følgende er beskrevet, hvem der har ansvar for hvad.

Databehandleren underretter den dataansvarlige
Hvis ScanNet mistænker, at der er sket et brud på persondatasikkerheden, vil ScanNet igangsætte en undersøgelse af grundlaget for mistanken, og såfremt der er sket et persondatalæk, vil ScanNets beredskabsorganisation blive aktiveret. Herefter vil ScanNet uden unødig forsinkelse, og inden for 48 timer, informere de berørte dataansvarlige webshopkunder.

Den dataansvarlige underretter Datatilsynet
Hvis der sker et læk af persondata, skal den dataansvarlige informere Datatilsynet herom. Den indledende rapport til Datatilsynet inden for de første 72 time skal indeholde en beskrivelse af:

- Hvilken type af brud du ved/mistænker har fundet sted;
- Antallet af registrerede, der muligvis er i fare;
- Hvilken risiko bruddet indebærer (for de berørte personer);
- Hvilke foranstaltninger der allerede er truffet på tidspunktet for indsendelse af rapporten;
- Og de foranstaltninger, du påtænker at træffe, men endnu ikke har truffet.

Hvis lækket ikke er sket hos jeres virksomhed, vil de oplysninger, som skal gives til Datatilsynet, som udgangspunkt fremgå af den underretning, som du får fra ScanNet.

Kontaktinformation for Datatilsynet
Datatilsynet kan kontaktes på følgende e-mailadresse: dt@datatilsynet.dk

Datatilsynet vil oprette en anmeldelsesformular på www.virk.dk, hvor anmeldelser om databrud skal ske.

Underretning om brud på persondatasikkerheden til datasubjektet
Denne underretningspligt gælder, hvis bruddet sandsynligvis vil indebære en høj risiko for den registreredes rettigheder i form af f.eks. identitetstyveri eller svindel, skade på omdømme, økonomisk ulempe m.fl.

Igen er det den dataansvarlige, der har underretningspligten. Så hvis du vurderer, at bruddet vil betyde risiko for ovenstående for dine kunder, så skal de underrettes om bruddet.

I kan finde inspiration til en beredskabsplan her:
Beredskabsplan og tjekliste i anledning af datalæk

ScanNet

10. Overførsel til tredjelande

Tredjelande er alle lande, som ikke er medlem af EU eller EØS (Island, Liechtenstein og Norge). Der er ikke noget forbud mod at overføre persondata til tredjelande. Det er bare noget mere besværligt, fordi GDPR stiller nye krav til, hvornår du lovligt kan overføre persondata til et tredjeland.

Hvorfor? Fordi GDPR kræver, at en virksomhed som overfører persondata til lande uden for EU, ikke må stille datasubjektet dårligere, end hvis virksomheden tilsvarende overfører til et land inden for EU. Derfor skal du være helt sikker på, at der er krav om lige så høj behandlingssikkerhed i tredjelandet, som der er inden for EU.

Hvordan gør jeg? Først og fremmest skal du være klar over, at der findes en række lande, som betegnes som sikre tredjelande.

Oversigt over sikre tredjelande:
Andorra, Argentina, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz og Uruguay.

Oversigt over sikre områder/sektorer i tredjelande:

Australien	Overførsel af oplysninger om flypassagerer
Canada	Modtagere underlagt den canadiske Personal Information Protection and Electronic Documents Act (PIPED ACT))
USA	Overførsel af oplysninger om flypassagerer, og overførsel til organisationer/virksomheder, der har tilsluttet sig EU-U.S. Privacy

Som udgangspunkt kan du uden videre overføre persondata til de sikre tredjelande og de sikre områder/sektorer i tredjelande, naturligvis forudsat at du har et formål og en grund til det. (Vær opmærksom på, at listen kan ændre sig)

Alle andre lande er usikre tredjelande, så hvis du vil overføre persondata hertil, så skal du have rigtig godt styr på din behandlingshjemmel og din dokumentation. Der skal enten gives fornødne garantier for en sikker databeskyttelse ved:

- Overførsel til Privacy Shield-certificerede virksomheder i USA (indtil videre) – man kan finde en liste over de virksomheder, der har tiltrådt EU-US Privacy Shield her: Privacy Shield
- Standardbestemmelser godkendt af Kommissionen (Standard Contractual Clauses) (indtil videre)
- Bindende virksomhedsregler (BCR)

Ellers kan du undtagelsesvis bruge følgende muligheder, hvis:

- Der foreligger udtrykkeligt samtykke fra datasubjektet
    - Der skal gives information om mulig risiko ved et utilstrækkeligt beskyttelsesniveau
- Det er nødvendigt for opfyldelse af en kontrakt
- Det er nødvendigt af hensyn til vigtige samfundsinteresser, retskrav eller vitale interesser
  Der er tale om et enkeltstående, begrænset tilfælde, hvor vægtige legitime interesser taler herfor (mere teoretisk end praktisk).

Når vi skriver "undtagelsesvis", skyldes det, at du kun har mulighed for at bruge ovenstående som grundlag for overførsler i begrænset omgang. Hvis du derfor i forbindelse med din forretning i væsentlig grad overfører persondata til tredjelande, så vil vi foreslå en gennemlæsning af Datatilsynets vejledning om overførsel af personoplysninger til tredjelande. Den kan findes her: Vejledning om overførsel af personoplysninger til tredjelande

ScanNets konklusion er, at hvis du kan finde en lige så god leverandør (databehandler) i EU som uden for EU, så sparer du noget arbejde ved at vælge den europæiske leverandør. Men hvis du vælger en leverandør uden for EU, så sørg for at have en veldokumenteret politik herom.

ScanNet