Nedenfor finder i et udkast til en procedure for håndtering af brud på persondatasikkerheden i jeres golfklub. Teksten er temmelig juridisk, men proceduren afspejler langt hen ad vejen de lovtekster der gælder for denne procedure, hvorfor den er beholdt i et meget juridisk sprog.

Alle tekster anført i [p*arenteser og med* *kursiv tekst]* er tænkt som hjælpetekster til inspiration til, hvad der skal overvejes og skrives. I skal gå ind og rette alle disse tekster, så de indeholder den tekst, der er rigtig for netop jeres golfklub.

Sidst i dokumentet følger udkast til den log, som I med fordel kan bruge til at registrere alle (store som små sikkerhedsbrud i jeres golfklub.

**-----**

**Procedure og log for håndtering af underretning af brud på persondatasikkerheden i [*indsæt navn på golfklub*]**

# INDLEDNING

[*Indsæt navn på golfklub*] er som dataansvarlig forpligtet til at underrette Datatilsynet i tilfælde af brud på persondatasikkerheden, jf. persondataforordningens artikel 33.

Underretningen kan undlades hvis det er usandsynligt, at hændelsen vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder. I sådanne situationer er [*Indsæt navn på golfklub*] ansvarlig for at kunne dokumentere, at virksomheden er bekendt med hændelsen, og at betingelserne for at undlade at underrette Datatilsynet er opfyldt.

Derfor skal alle brud på persondatasikkerheden dokumenteres, så den valgte handlingsmåde kan dokumenteres, hvis Datatilsynet stiller spørgsmål.

Hvis hændelsen medfører en høj risiko for fysiske personers rettigheder og frihedsrettigheder skal [*Indsæt navn på golfklub*] ud over at underrette Datatilsynet også underrette de registrerede.

Risiciene for fysiske personers rettigheder og frihedsrettigheder kan opstå som følge af:

* fysisk, materiel eller immateriel skade
* identitetstyveri eller -svig, finansielle tab, skade på omdømme
* tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt
* uautoriseret ophævelse af pseudonymisering
* andre betydelige økonomiske eller sociale konsekvenser
* de registrerede berøves deres rettigheder og frihedsrettigheder
* de registrerede forhindres i at udøve kontrol med deres personoplysninger
* der behandles personoplysninger, der viser race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, og behandling af genetiske data, helbredsoplysninger eller oplysninger om seksuelle forhold eller straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger
* personlige forhold evalueres, navnlig analyse eller forudsigelse af forhold vedrørende indsats på arbejdspladsen, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografisk position eller bevægelser, med henblik på at oprette eller anvende personlige profiler
* der behandles personoplysninger om sårbare fysiske personer, navnlig børn
* behandlingen omfatter en stor mængde personoplysninger og berører et stort antal registrerede.

## Hvad er et "brud på persondatasikkerheden"?

Et brud på persondatasikkerheden er defineret i persondataforordningens artikel 4(2) som "et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet".

Det er vigtigt, at alle medarbejdere er i stand til at identificere et brud på persondatasikkerheden og ved, hvordan en sådan hændelse skal håndteres.

Derudover skal de personer, der påtænkes involveret i håndteringen af et brud på persondatasikkerheden, være uddannet i procedurerne for håndtering af sådanne hændelser.

## Tidsfrister

Datatilsynet skal informeres uden unødig forsinkelse og inden for 72 timer. Orienteringen sker digitalt på Datatilsynets hjemmeside eller på[www.virk.dk](http://www.virk.dk).

Der er ingen fast tidsfrist for underretning af de registrerede - timingen af denne underretning afhænger af de mulige konsekvenser for de registrerede, og der kan være krav om meget hurtig underretning.

Information kan gives gradvist i takt med at sagen undersøges.

# Procedure

Når der rapporteres om et brud på persondatasikkerheden skal denne procedure følges:

|  |  |  |
| --- | --- | --- |
|  | **Aktivitet** | **Bemærkninger** |
| 1 | Opret en hændelse i loggen, som du får udleveret ved at henvende dig til direktionssekretariatet. Alle efterfølgende handlinger skal ligeledes dokumenteres i loggen. | Ethvert brud på persondatasikkerheden skal dokumenteres, jf. artikel 33 (5).  Som udgangspunkt skal Datatilsynet underrettes om brud på persondatasikkerheden inden for 72 timer fra det tidspunkt, hvor [*Indsæt navn på golfklub*] er blevet bekendt med hændelsen (med mindre det er usandsynligt at hændelsen medfører en risiko for fysiske personers rettigheder og frihedsrettigheder).  Tidsfristen på 72 timer regnes fra det tidspunkt hvor den første person i [*Indsæt navn på golfklub*] er blevet bekendt med hændelsen. Det er derfor vigtigt, at dette tidspunkt registreres.  Derudover bør følgende information indsamles i det omfang, det er muligt på nuværende tidspunkt:   * Identitet og kontaktinformation for den person, der har rapporteret hændelsen * En beskrivelse af hændelsen (f.eks. stjålet pc, mistet USB-stik, fejlsendt e-mail, hacking) * Hvem (registrerede) er berørt af hændelsen * Hvilke informationer er omfattet af hændelsen |
| 2 | Indkald kriseteam | Kriseteamet bør som minimum omfatte repræsentanter for   * [*Bestyrelsen]* * [*Sekretariatet]*   Kriseteamet beslutter, hvordan situationen skal håndteres. Kriseteamet arbejder tæt sammen de næste par døgn i forhold til at overholdes tidsfristen for orientering til Datatilsynet (inden 72 timer). |
| 3 | Underret (hvis relevant):   * Datatilsynet * De registrerede | Se punkt 4 og 5 for yderligere vejledning |
| 4 | Underret Datatilsynet (hvis relevant) | Datatilsynet skal underrettes med mindre det er usandsynligt at bruddet på persondatasikkerheden vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder.  Underretningen til Datatilsynet skal som minimum omfatte følgende information:   * Den dataansvarliges identitet (*Indsæt navn på golfklub*) * Kontaktinformationer for kontaktperson hos den dataansvarlige * Beskrivelse af hændelsen * Antal registrerede der er berørt af hændelsen (hvis antallet kendes) * Kategorierne af registrerede, der er berørt af hændelsen * Kategorierne af personoplysninger, der er omfattet af hændelsen * Hændelsens sandsynlige konsekvenser for de registrerede * Afhjælpende foranstaltninger der er iværksat * Planer for videre håndtering af situationen   Information til Datatilsynet kan gives løbende i takt med, at [*Indsæt navn på golfklub*] bliver bekendt med informationen.  Giv derfor kun bekræftet, faktuel information. Hvis det skønnes relevant at oplyse om formodninger skal det gøres klart, hvad der er faktum og hvad der er formodninger.  UNDLAD AT GÆTTE ELLER FREMSÆTTE UUNDERBYGGEDE TEORIER |
| 5 | Underret de registrerede (hvis relevant) | **Hvornår er der pligt til at underrette de registrerede:**  Om - og i givet fald hvornår - de registrerede skal underrettes afhænger af den risiko, hændelsen medfører for de registrerede.  Der er alene pligt til at informere de registrerede, hvis hændelsen medfører en høj risiko for de registreredes rettigheder og frihedsrettigheder, f.eks.   * identitetstyveri * økonomisk tab eller tab af omdømme * kompromittering af fortroligheden for oplysninger, der er omfattet af lovbestemt tavshedspligt * den registrerede fratages rettigheder eller frihedsrettigheder eller hinders adgang til at udøve kontrol over deres data   Ovenstående er kun eksempler og udgør således ikke en udtømmende liste.  Undtagelser til underretningspligten:  Pligten til at underrette de registrerede finder ikke anvendelse, jf. artikel 34 (3), hvis   * 1. den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering   2. den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder sandsynligvis ikke længere er reel   3. det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.   Derudover fremgår det af databeskyttelseslovens § 22, stk. 1, at forpligtelsen til at underrette de registrerede efter persondatafororodningens artikel 34 ikke skal gælde, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv.  Ligeledes fremgår det af databeskyttelseslovens § 22, stk. 6, at forpligtelsen til at underrette de registrerede efter persondatafororodningens art. 34 ikke skal gælde, hvis underretning af de registrerede må antages at vanskelligøre efterforskningen af strafbare forhold. Det er kun politiet, der kan gøre brug af denne undtagelse.  **Hvem af de registrerede skal underrettes:**  Hvis der er pligt til at underrette de registrerede, skal der ske underretning af alle, der ikke positivt kan fastslås ikke at være berørt af hændelsen. Ordvalget i underretningen skal tydeligt afspejle om modtageren   * med sikkerhed er berørt; * formodes at være berørt, eller * "bare" ikke med sikkerhed kan siges ikke at være berørt.   **Hvornår skal de registerede underrettes:**  De registrerede skal underrette uden unødig forsinkelse.  Hovedreglen er, at jo større risiko de registrerede er udsat for som følge af hændelsen, desto hurtigere skal de underrettes, så de har mulighed for aktivt at hindre risikoen i at materialisere sig, subsidiært at begrænse de negative konsekvenser. Eksempelvis vil det kræve en meget hurtig reaktion, hvis bankkunders bruger-id og password til en netbank-løsning kompromitteres.  I sådanne situationer skal underretningen til de registrerede - ud over en beskrivelse af faktuelle forhold - indeholde anbefalinger til, hvordan den registrerede kan nedbringe risikoen for negative konsekvenser af hændelsen.  **Hvordan skal de registrerede informeres:**  Underretningen af de registrerede skal - som minimum - indeholde følgende information:   * Den dataansvarliges identitet * Kontaktinformationer for kontaktperson hos den dataansvarlige * Beskrivelse af hændelsen * Beskrivelse af hvilke data, der er kompromitteret * Hændelsens mulige konsekvenser for de registrerede * Afhjælpende foranstaltninger der er iværksat * Beskrivelse af foranstaltninger, den registrerede selv bør iværksætte   Underretningen skal gives i et "klart og forståeligt sprog".  For at undgå unødig bekymring blandt de registrerede bør underretningen indeholde klar og utvetyding information om, hvorvidt den registrerede   * med sikkerhed er berørt; * formodes at være berørt, eller * "bare" ikke med sikkerhed kan siges ikke at være berørt. |
| 6 | Giv opdateret information til Datatilsynet og/eller de registrerede (hvis relevant) | Hvis virksomheden bliver bekendt med ny, relevant information, kan der være behov for at informere Datatilsynet og/eller de registrerede. |
| 7 | Gennemfør "lessons learned" | Når kriseteamet beslutter, at sagen kan lukkes, bør der gennemføres et "lessons learned" forløb for at sikre, at relevant viden opsamles - både i forhold til forbedring af proceduren og i forhold til at undgå lignende hændelser fremover. |
| 8 | Luk sagen |  |

# YDERLIGERE VEJLEDNING

Yderligere vejledning kan findes i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden samt vejledning fra det Europæiske Databeskyttelsesråd.

Grundet den dynamiske natur af og for informationer og informationssikkerhed bør hver hændelse vurderes konkret og i lyset af risikoscenariet på det tidspunkt, hvor hændelsen finder sted.

# Referencer

Persondataforordningen

- Artikel 33 og 34

- Betragtningerne 75, 85, 86, 87 og 88

Databeskyttelsesloven § 22, stk. 1 og stk. 6

Datatilsynets vejledning om håndtering af brud på persondatasikkerheden

LOG til brug ved brud på datasikkerheden i [*indsæt navn på golfklub*]

Hjælp kan hentes i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden

|  |  |  |
| --- | --- | --- |
|  | **Brud på persondatasikkerheden** | **Beskrivelse af bruddet** |
| 1. | Angiv navn og kontaktinfo på den, der opdagede bruddet: |  |
| 2. | Angiv dato og tidspunkt for bruddet: |  |
| 3. | Hvad er der sket? |  |
| 4. | Angiv årsagen til bruddet: |  |
| 5. | Hvilke kategorier af personoplysninger er berørt? |  |
| 6. | Hvilke konsekvenser har bruddet for de berørte personer? |  |
| 7. | Hvilke afhjælpende foranstaltninger er truffet? |  |
| 8. | Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår?)? |  |
| 8.1 | (Hvis nej under 7.) Begrundelse for ikke at anmelde bruddet til Datatilsynet: |  |
| 9. | Er der sket underretning af de berørte personer (hvis ja, hvornår?)? |  |
| 9.1 | (Hvis nej under 8.) Begrundelse for ikke at underrette de berørte personer: |  |

|  |  |  |
| --- | --- | --- |
|  | **Brud på persondatasikkerheden** | **Beskrivelse af bruddet** |
| 1. | Angiv navn og kontaktinfo på den, der opdagede bruddet: |  |
| 2. | Angiv dato og tidspunkt for bruddet: |  |
| 3. | Hvad er der sket? |  |
| 4. | Angiv årsagen til bruddet: |  |
| 5. | Hvilke kategorier af personoplysninger er berørt? |  |
| 6. | Hvilke konsekvenser har bruddet for de berørte personer? |  |
| 7. | Hvilke afhjælpende foranstaltninger er truffet? |  |
| 8. | Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår?)? |  |
| 8.1 | (Hvis nej under 7.) Begrundelse for ikke at anmelde bruddet til Datatilsynet: |  |
| 9. | Er der sket underretning af de berørte personer (hvis ja, hvornår?)? |  |
| 9.1 | (Hvis nej under 8.) Begrundelse for ikke at underrette de berørte personer: |  |

|  |  |  |
| --- | --- | --- |
|  | **Brud på persondatasikkerheden** | **Beskrivelse af bruddet** |
| 1. | Angiv navn og kontaktinfo på den, der opdagede bruddet: |  |
| 2. | Angiv dato og tidspunkt for bruddet: |  |
| 3. | Hvad er der sket? |  |
| 4. | Angiv årsagen til bruddet: |  |
| 5. | Hvilke kategorier af personoplysninger er berørt? |  |
| 6. | Hvilke konsekvenser har bruddet for de berørte personer? |  |
| 7. | Hvilke afhjælpende foranstaltninger er truffet? |  |
| 8. | Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår?)? |  |
| 8.1 | (Hvis nej under 7.) Begrundelse for ikke at anmelde bruddet til Datatilsynet: |  |
| 9. | Er der sket underretning af de berørte personer (hvis ja, hvornår?)? |  |
| 9.1 | (Hvis nej under 8.) Begrundelse for ikke at underrette de berørte personer: |  |

Indsæt nye logfelter, når de første er udfyldt.

|  |  |  |
| --- | --- | --- |
|  | **Brud på persondatasikkerheden** | **Beskrivelse af bruddet** |
| 1. | Angiv navn og kontaktinfo på den, der opdagede bruddet: |  |
| 2. | Angiv dato og tidspunkt for bruddet: |  |
| 3. | Hvad er der sket? |  |
| 4. | Angiv årsagen til bruddet: |  |
| 5. | Hvilke kategorier af personoplysninger er berørt? |  |
| 6. | Hvilke konsekvenser har bruddet for de berørte personer? |  |
| 7. | Hvilke afhjælpende foranstaltninger er truffet? |  |
| 8. | Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår?)? |  |
| 8.1 | (Hvis nej under 7.) Begrundelse for ikke at anmelde bruddet til Datatilsynet: |  |
| 9. | Er der sket underretning af de berørte personer (hvis ja, hvornår?)? |  |
| 9.1 | (Hvis nej under 8.) Begrundelse for ikke at underrette de berørte personer: |  |