Tillæg om persondatabeskyttelse på HackerStop-platformen

Tillæg om databeskyttelse udgør en del af den Licensaftale, der er indgået mellem Dansk IT og den part, der anvender HackerStop.dk (herefter Kunden). Kunden betragtes som dataansvarlig for behandlingen af de persondata på HackerStop-platformen, der er knyttet til Kunden og dennes brugere.

Parterne aftaler, at dette Tillæg om persondatabeskyttelse på HackerStop-platformen angiver deres forpligtelser for så vidt angår behandlingen og sikkerheden af de persondata, der behandles af Dansk IT ("databehandleren") på vegne af Kunden ("den dataansvarlige") som led i dennes brug af HackerStop-platformen.

Dansk IT påtager sig som databehandler forpligtelserne i dette Tillæg om persondatabeskyttelse over for alle Kunder med licensaftaler til HackerStop.dk.

I tilfælde af konflikt eller uoverensstemmelse mellem vilkårene i Tillæg om databeskyttelse og andre vilkår i Serviceaftalen, har Tillæg om databeskyttelse forrang. Bestemmelserne i vilkårene for Tillæg om databeskyttelse træder i stedet for eventuelle uoverensstemmende bestemmelser i Dansk IT's Politik om beskyttelse af personoplysninger, der ellers gælder for behandlingen af persondata på Dansk IT's platforme.

Er der spørgsmål om persondatabeskyttelse og behandlingssikkerhed på HackerStop-platformen, kan Dansk IT kontaktes ved brug af nedenstående kontaktoplysninger:

Dansk IT
Vermundsgade 38A, st. Tv.
2100 København Ø Danmark
CVR 83973315

Kontaktperson for persondatabeskyttelse:

Navn: Claudia Zöllner

Mail: Hackerstop@dit.dk

Indhold

1. Præambel 3

2. Den dataansvarliges rettigheder og forpligtelser 4

3. Databehandleren handler efter instruks 4

4. Fortrolighed 4

5. Behandlingssikkerhed 4

6. Anvendelse af underdatabehandlere 5

7. Overførsel til tredjelande eller internationale organisationer 6

8. Bistand til den dataansvarlige 7

9. Underretning om brud på persondatasikkerheden 8

10. Sletning og returnering af oplysninger 8

11. Revision, herunder inspektion 8

12. Parternes aftale om andre forhold 9

13. Ikrafttræden og ophør 9

14. Kontaktpersoner hos databehandleren 9

Bilag A Oplysninger om behandlingen 10

Bilag B Underdatabehandlere 11

Bilag C Instruks vedrørende behandling af personoplysninger 12

1. Præambel

1.1 Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

1.2 Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

1.3 I forbindelse med leveringen af HackerStop-platformen behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

1.4 Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder de almindelige betingelser og vilkår for brug af HackerStop-platformen.

1.5 Der hører tre bilag til disse Bestemmelser (Bilag A, B, og C), og bilagene udgør en integreret del af Bestemmelserne.

1.6 Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

1.7 Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

1.8 Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

1.9 Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

1.10 Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

2. Den dataansvarliges rettigheder og forpligtelser

2.1 Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2.2 Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

2.3 Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

3. Databehandleren handler efter instruks

3.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i Bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

3.2 Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

4. Fortrolighed

4.1 Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

4.2 Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

5. Behandlingssikkerhed

5.1 Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder,

[1] Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a. Pseudonymisering og kryptering af personoplysninger

b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

5.2 Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

5.3 Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i Bilag C.

6. Anvendelse af underdatabehandlere

6.1 Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 14 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i Bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af Bilag B.

6.2 Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske

og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

6.3 Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår,

som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6.4 Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

6.5 Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

7. Overførsel til tredjelande eller internationale organisationer

7.1 Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

7.2 Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

7.3 Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

c. behandle personoplysningerne i et tredjeland

7.4 Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i Bilag C.6.

7.5 Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

8. Bistand til den dataansvarlige

8.1 Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a. Oplysningspligten ved indsamling af personoplysninger hos den registrerede

b. Oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

c. Indsigtsretten

d. Retten til berigtigelse

e. Retten til sletning (”retten til at blive glemt”)

f. Retten til begrænsning af behandling

g. Underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

h. Retten til dataportabilitet

i. Retten til indsigelse

8.2 I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 5.3, bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

a. Den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

b. Den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

c. Den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. Den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

Parterne skal i Bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 8.1 og 8.2.

9. Underretning om brud på persondatasikkerheden

9.1 Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

9.2 Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

9.3 I overensstemmelse med Bestemmelse 8.2.1 skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

9.4 Parterne skal i Bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

10. Sletning og returnering af oplysninger

10.1 Ved ophør af tjenesterne vedrørende behandling af virksomhedsoplysninger, er databehandleren forpligtet til at slette alle virksomhedsoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

10.2. Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

11. Revision, herunder inspektion

11.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der

foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

11.2 Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7 og C.8.

11.3 Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

12. Parternes aftale om andre forhold

12.1 Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

13. Ikrafttræden og ophør

13.1 Bestemmelserne træder i kraft på datoen for brugeren ibrugtagning af HackerStop.

13.3 Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

13.4 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet i overensstemmelse med Bestemmelse 10.1 og Bilag C.4 anses Bestemmelserne som ophørt.

14. Kontaktpersoner hos databehandleren

Navn: Claudia Zöllner

Stilling: Projektleder, HackerStop

Mail: Hackerstop@dit.dk

Tlf.nr: +45 33 11 15 60

Bilag A Oplysninger om behandlingen

A.1 Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige:

At den dataansvarlige kan udbyde HackerStop-platformen, som ejes og administreres af databehandleren, til at indsamle og behandle oplysninger om de HackerStop-brugere, der gives adgang til HackerStop-platformen af den dataansvarlige.

A.2 Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige omfatter

Behandling af de persondata, som behandles som led i tilpasning af HackerStop-platformen, herunder af database og applikationer, til kundens behov samt behandling af de persondata, der indtastes af kunden eller dennes brugere som led i anvendelsen af HackerStop-platformen

A.3 Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Kontaktoplysninger, herunder navn, e-mail.

Personlige oplysninger, herunder stilling, køn og land.

Oplysninger om erfaringer, vaner, rutiner mv. om informationssikkerhed og brug af it-udstyr.

I særlige tilfælde kan behandlingen omfatte særlige kategorier af personoplysninger (følsomme oplysninger), da det er muligt for brugere af platformen selv at tilføje spørgsmål og kommentarer. Følsomme oplysninger vil kunne forekomme, hvis de indgår i brugerens brug af fritekstfelter.

A.4 Behandlingen omfatter følgende kategorier af registrerede

Personer, som har oprettet en HackerStop profil på Hackerstop-platformen

Virksomhedsrepræsentanter, der har oprettet en virksomhedsprofil på platformen

A.5 Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed:

Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne. Databehandleraftalen skal ophæves separat fra parternes kommercielle aftale.

Bilag B Underdatabehandlere

B.1 Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere.

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Microsoft Datacenter Netherlands B.V.	NL34143486	Evert van de Beekstraat 354, 1118 CZ, Luchthaven Schiphol, Noord-Holland, Netherlands	Server hosting GDPR info: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Azure
Brevo (SendInBlue)	FR80498019298	Sendinblue SAS 7 rue de Madrid, 75008 Paris, France	Email gateway GDPR info: https://help.brevo.com/hc/en-us/articles/360001258744-How-does-Brevo-comply-with-the-GDPR
MongoDB	IE9793087U	3 Shelbourne Building, 3rd Floor Crampton Avenue, Ballsbridge, Dublin 4 Ireland	Database hosting GDPR info: https://www.mongodb.com/legal/privacy

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandler for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1 Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Databehandleren understøtter HackerStop-platformen med database og applikationer, og foretager som led heri tilpasning, drift og vedligehold af Hackerstop.dk og den underliggende platform. Dette omfatter indsamling, behandling og opbevaring af persondata på vegne af den dataansvarlige

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle den risiko, der er forbundet med at behandle personoplysningerne i HackerStop-platformen i forhold til de registreredes rettigheder og frihedsrettigheder. Niveauet skal fastlægges under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt sandsynligheden for at behandlingen medfører negative konsekvenser for de registrerede. Det skal indgå i vurderingen, at HackerStop-platformen vil kunne indeholde særlige kategorier af personoplysninger, som er omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", eller kan anses som fortrolige. Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog - i alle tilfælde og som minimum - gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige (på baggrund af den risikovurdering den dataansvarlige har foretaget):

Pseudonymisering og anonymisering

- Personoplysninger anonymiseres, når en bruger slettes efter anmodning eller ved aftalens ophør.

Sikkerhed, fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester

- Servere opdateres i forbindelse med løbende releases
- Database og applikation er hosted hos Networked Business Institute ApS, Frederiksberg, Danmark
- Der benyttes SSL kryptering i al dialog imellem database og applikation samt imellem bruger og systemet.
- Al transmission til underdatabehandlerens anvendte tredjeparter krypteres
- Ved opbevaring af persondata fra Hackerstop-platformen i Cloud data anvendes kryptering
- Krypteringsnøgler til opbevaring i Cloud opbevares hos en uafhængig tredjepart indenfor EU.

Genopretning og tilgængelighed

- Der foretages automatiseret realtime backup af databasen med point-in-time restore de seneste 24 timer og periodiske fulde backups der gemmes i op til 2 år.

- Database og applikation er driftet med fuldt automatiseret monitorering og redundans. Ved fejl på underliggende hardware skiftes automatisk til sunde instanser i andre zoner. Fejlende instanser genskabes og reintroduceres automatisk.
- Database og applikation skalerer automatisk kapaciteten efter den registrerede load.

Revision og sikring af overholdelse

- Alle procedurer for driften af HackerStop-platformen evalueres og kontrolleres årligt.

Beskyttelse mod uberettiget tilgang

- Al adgang til persondata på Hackerstop-platformen er baseret på authentication på API niveau. Ved login tildeles midlertidig authentication token, der benyttes ved alle API forespørgsler.
- Ingen slutbruger eller bruger hos den dataansvarlige har adgang til databasen. Administrativ databaseadgang er beskyttet af SSL og IP-filtrering og foretages kun af platformsleverandøren for udvikling og support.
- Slutbrugerne tilgår applikationen via SSL over internettet uden IP-filtrering eller VPN. Der er ingen forskel i adgangen fra kontorarbejde og hjemmearbejde.
- Den fysiske beskyttelse af data er baseret på Microsoft Azure datacentrenes fysiske sikkerhed som er nærmere beskrevet her: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Logning

- Tilgang til persondata via HackerStop-platformen logges via webserver adgangslog med IP, tidspunkt og forespørgsel inkl. authentication token. Log gemmes i min. 30 dage.
- Administrativ tilgang til databasen logges med IP, tidspunkt og brugernavn. Log gemmes i 7 dage.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- Sletning af personoplysninger på dataansvarliges eller registreredes anmodning
- Mulighed for udtræk af registreredes oplysninger på dataansvarliges eller registreredes anmodning
- Nødvendige oplysninger til den dataansvarlige og registrerede for at overholde oplysningspligten
- I tilfælde af brud på persondatasikkerheden skal databehandleren bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden. Denne information vil blive offentliggjort på hackerstop.dk.

C.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette personoplysningerne i overensstemmelse med bestemmelse 11.1 og 11.2, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne

C.5 Lokalitet for behandling

Behandling af de i aftalen omfattede personoplysninger sker på de lokaliteter, der er nævnt i Bilag B samt hos de databehandlere, som benyttes af underdatabehandleren. samt dennes eventuelle underdatabehandlere.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Der kan alene overføres personoplysninger til tredjelande efter skriftlig godkendelse fra den dataansvarlige.

Overførsel til tredjelande kan alene ske i overensstemmelse med databeskyttelsesforordningens kapitel V og vejledning fra Det Europæiske Databeskyttelsesråd (EDPB).

Overførsler kan kun foretages på baggrund af EU Kommissionens afgørelse om tilstrækkeligt sikkerhedsniveau (sikre tredjelande) eller ved anvendelse af EU Kommissionens Standard Contractual Clauses on data transfers between EU and non-EU countries som overførselsgrundlag.

Forud for en overførsel, undersøger databehandleren, om der er behov for at fastsætte krav om supplerende tekniske foranstaltninger, som sikrer et beskyttelsesniveau, der i det væsentlige svarer til niveauet indenfor EU/EØS.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Den dataansvarlige eller en repræsentant for denne kan gennemføre en årlig skriftlig kontrol med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Baseret på en vurdering af den skriftlige besvarelse samt en risikovurdering af behandlingsaktiviteterne kan en gennemført skriftlig kontrol suppleres med en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

Databehandleren udarbejder uden vederlag årligt en erklæring, en IT-sikkerhedsinspektion, der bekræfter, at databehandleren fortsat efterlever alle krav i disse Bestemmelser.

C.8 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandlere

Databehandleren eller en repræsentant for denne gennemfører årligt en skriftlig kontrol med henblik på at fastslå anvendte underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Baseret på en vurdering af den skriftlige besvarelse samt en risikovurdering af behandlingsaktiviteterne kan den skriftlige kontrol suppleres med en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Databehandleren bærer eventuelle omkostninger i forbindelse med tilsyn hos underdatabehandlere.