SIXTUS

VIRKSOMHED

Inspektionsrapport vedr. databehandleraftale med Dansk IT´s Hackerstop kunder

29. Januar 2024

Store Regnegade 2 · 1110 København
Tlf.: +45 30 65 43 35 · CVR: 40649832
info@sixtus-compliance.dk · sixtus-compliance.dk

SIXTUS

Indholdsfortegnelse

Store Regnegade 2 · 1110 København
Tlf.: +45 30 65 43 35 · CVR: 40649832
info@sixtus-compliance.dk · sixtus-compliance.dk

SIXTUS

Ledelsens udtalelse

Dansk IT behandler personoplysninger på vegne af den dataansvarlige i henhold til databehandleraftale indgået mellem parterne.

Medfølgende beskrivelse og inspektionsrapport er udarbejdet til brug for den dataansvarlige, der har anvendt Dansk IT services i deres Hackerstop platform, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Dansk IT bekræfter, at nedenstående beskrivelse, giver en retvisende beskrivelse af Dansk IT, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i henhold til den indgåede databehandleraftale.

Vurdering

Dansk IT har vurderet en samlet lav risiko i forbindelse med behandlingen af de henførbare data. Dette er vurderet ud fra at Dansk IT stiller en platform til rådighed, hvor der kun anvendes login oplysninger fra virksomheder og dennes medarbejdere, og har derfor ingen eller meget få og kun almindelige henførebare personoplysninger, og at disse benyttes primært til login på løsningen. Der kan findes følsomme data, men da dette er i virksomhedens egen instans, har Dansk IT ingen kontrol over dette. Det er desuden ikke Dansk ITs formål at behandle disse oplysninger.

Inspektørens udtalelse

Omfang

Sixtus Compliance har fået til opgave at inspicere og rapportere vedr. Dansk IT's beskrivelse af ydelsen i henhold til indgåede databehandleraftaler med kunder sammenholdt med udformningen og funktionen af kontroller, der knytter sig til databehandleraftalen.

Inspektionsperioden er 27 januar 2023 til 30 januar 2024

Inspektionen udføres for at sikre, at databehandlingen efterlever de tekniske og organisatoriske sikkerhedsforanstaltninger, der er angivet i databehandleraftalen samt databehandlerens generelle forpligtelser.

Regelgrundlag

Regelgrundlaget for inspektionen af behandlingssikkerheden er databeskyttelsesforordningens artikel 28, hvorefter en dataansvarlig "*udelukkende benytter databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder*".

Bestemmelsen er udmøntet i Datatilsynets standard databehandleraftale bilag C "Instruks vedrørende behandling af personoplysninger".

SIXTUS

Ansvar og fremgangsmåde

Vores ansvar er at inspicere og rapportere Dansk IT's implementering af forhold, der er beskrevet i databehandleraftalen, herunder generelle forpligtelser for databehandlere, tekniske sikkerhedsforanstaltninger og organisatoriske sikkerhedsforanstaltninger.

Inspektionen omfatter bl.a. interviews, stikprøver og tests, og er udført med udgangspunkt i almindeligt accepterede metoder og politikker for interne audits.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for inspektionsrapporten og vores udtalelse.

Sixtus Compliance ApS
Store Regnegade 2
1110 København K

Dato: 29/01/2024

Bo Pyskow

Dansk IT
Vermundsgade 38A st.tv
2100 København Ø

Dato: 29.01.2024

Jeanette Hartz

SIXTUS

Beskrivelse af behandling og omfang

Karakteren af behandlingen

Der behandles personhenførbare data i forbindelse med kundernes brug af Hackerstop platformen.

Formålet med platformen er at skabe kontinuerlig awareness og hjælpe virksomheder til at skabe en sikker digital adfærd på arbejdspladsen.

Såfremt Dansk IT involveres i en problemløsning på kundens systemer, foretages rådgivning uden direkte behandling af kunde data. I de tilfælde hvor de ikke kan undgås at have adgang til kundedata sker det under accept og vejledning fra kunderne.

I de tilfælde hvor Kunden anmoder Dansk IT om at foretage analyser af de allerede eksisterende forretningsmæssige data angiver Kunden hvilke typer af analyser de ønsker at få foretaget. Dette foretages kun på anonymiseret data, der udleveres af kunden.

Der er således ikke en direkte behandling data, men Dansk IT og dennes underleverandør, kan have kontakt med virksomhedernes og deres kunders data når der implementeres løsninger eller foretages support og problemløsning.

Personoplysninger

Den dataansvarlige indtaster kun almindelige personoplysninger (navn, adresse, e-mail, telefonnummer o.l.) på brugere, leverandører/samarbejdspartnere og evt. kunder (hvis dataansvarlige også agerer som databehandler).

Dansk IT indtaster eller behandler ikke kundens data uden for instruktion i de respektive Databehandleraftaler.

Praktiske tiltag

Der er implementeret passende tekniske og organisatoriske foranstaltninger til at sikker behandling af personoplysninger i form af politikker, processer og intern undervisning.

Disse tiltag er beskrevet i databehandleraftalen, og danner grundlag for denne inspektion.

Tekniske sikkerhedsforanstaltninger - underdatabehandlere

For så vidt angår databehandlerene Microsoft, Sociale Medier og andre understøttende systemer og interne værktøjer, som behandler persondata uden for EU, er det konstateret at disse understøtter det nye aftalte overførselsgrundlag imellem USA og EU; Data Privacy Framework.

Slettepolitik for dataansvarliges data

Den Dataansvarlige har selv kontrol over den data der ligger i deres løsning. Dansk IT modtager derfor intet personhenførbar data, som skal slettes eller leveres tilbage.

SIXTUS

Kontrolaktivitet og resultat

1. Generelle principper for databehandlere			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
1.1	Der føres årligt tilsyn med underdatabehandlere.	Inspektion af log over tilsyn med underdatabehandlere jf. pkt. B.2 Godkendte underdatabehandlere i databehandleraftalen	Ingen anmærkninger
1.2	Der er udarbejdet fortegnelse over dataansvarlige, til brug for information i tilfælde af brud på datasikkerheden.	Foretaget interview med medarbejder ansvarlig for fortegnelsen.	Ingen anmærkninger
1.3	Der er udarbejdet intern instruks for underretning af dataansvarlige i tilfælde af brud på datasikkerheden.	Vi har inspiceret instruksen for håndtering af brud på datasikkerheden	Ingen anmærkninger
1.4	Den dataansvarliges data slettes efter ophør af aftale	Vi har inspiceret at der er aftalt/informeret tidsramme for sletning af data efter abonnementsophør.	Ingen anmærkninger
1.5	Der er udarbejdet intern instruks for Data subjekters indsigtsanmodning	Vi har inspiceret instruksen for håndtering af indsigtsanmodninger	Ingen anmærkninger

2. Tekniske sikkerhedsforanstaltninger (Eksterne, interne applikationer)			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
2.1	SSL krypteret forbindelse med klient og server	Inspiceret at forbindelse mellem klient og server bliver etableret med kryptering	Ingen anmærkninger
2.2	2-faktor validering ved login på platformen	Inspiceret at login kræver 2-faktor validering	Der er ikke 2FA på Hacker Stop Platformen, men dette er implementeret på de underliggende platforme. Ingen anmærkninger
2.3	Adgangskode opbevares krypteret (128-bit kryptering)	Inspiceret opbevaring af adgangskode i database.	Ingen anmærkninger
2.4	Anerkendt hosting partner • ISO 27001 og ISAE 3402 T2 certificeret • Løbende backup og logning	Inspiceret at hosting partneren er ISO 27001 og ISAE 3402 T2 certificeret. Inspiceret dokumentation for backup fra hostingpartner	Ingen anmærkninger

2.5	Underdatabehandlere er i EU eller USA (Alle med lovligt grundlag for processering)	Inspiceret at underdatabehandlerne behandler data i EU eller i USA under SCC	Ingen anmærkninger
2.6	Driftsmiljøet er adskilt fra udviklings- og testmiljøer	Vi har foretaget interview med medarbejderne i udviklingen, samt inspiceret dokumentation.	Ingen anmærkninger
2.7	Kryptering af personoplysninger	Vi har inspiceret at: Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. Politikken definerer styrken og protokollen for kryptering. Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail.	Ingen anmærkninger
2.8	Fjernarbejdspladser og fjernadgang til systemer og data	Vi har inspiceret at: Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse ([SHA-2 & 256 bit]) Fjernadgang skal foregå via to-faktor autentifikation.	Ingen anmærkninger
2.9	Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger	Vi har inspiceret at: Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges. Alle brugerændringer i system og databaser logges. Loggen slettes efter den fastsatte retentionsperiode Databehandler monitorere og logger netværkstrafik. Databehandler opbevarer logs i X-år/X-måneder.	Ingen anmærkninger

SIXTUS

3. Tekniske sikkerhedsforanstaltninger (Interne)			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
3.1	Alle computere har opdateret antivirus	Inspiceret log for egenkontrol af intern sikkerhed.	Ingen anmærkninger
3.2	Firewalls på maskiner og forbindelser	Inspiceret log for egenkontrol af intern sikkerhed.	Ingen anmærkninger
3.3	Passwords udskiftes løbende	Inspiceret log for egenkontrol af intern sikkerhed.	Ingen anmærkninger
3.4	Løbende opdatering af operativsystemer og applikationer, herunder Java, Adobe, plugins mv.	Inspiceret log for egenkontrol af intern sikkerhed.	Ingen anmærkninger
3.5	Løbende backup	Inspiceret log for egenkontrol af intern sikkerhed.	Ingen anmærkninger

4. Organisatoriske sikkerhedsforanstaltninger			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
4.1	Alle med arbejdere er instrueret i beskyttelsen af personoplysninger og har underskrevet medarbejderinstruks. • Instruksen gennemgås og opdateres mindst en gang årligt. • Instruksen gennemgås med nye medarbejdere i forbindelse med ansættelsen.	Inspiceret log for gennemgang af medarbejderinstruks	Ingen anmærkninger
4.2	Alle medarbejdere hos DANSK IT er pålagt tavshedspligt	Inspiceret at ansættelsesaftaler angiver tavshedspligt.	Ingen anmærkninger

5. Fysiske sikkerhedsforanstaltninger			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
5.1	Kontorer og bygninger aflåses, når de forlades.	Foretaget interview med medarbejdere og gennemgået instruks for aflåsning af bygninger	Ingen anmærkninger
5.2	Evt. arkiver med følsomme personoplysninger opbevares altid aflåst	Foretaget interview med medarbejdere og gennemgået procedure for opbevaring af arkiver med følsomme personoplysninger	Ingen anmærkninger
5.3	Backup opbevares aflåst	Foretaget interview med backupansvarlig vedr. Backup-rutiner. Inspiceret backuprutiner for datacenter og ekstern backup	Ingen anmærkninger

SIXTUS

6. Driftsmæssig sikkerhed			
Nr.	**Kontrolpunkt**	**Udført test**	**Resultat af test**
6.1	Udvikling, Test og Produktionsmiljøer er adskilte. • Udvikling og test/kontrol foretages af forskellige personer.	Vi har foretaget interview med medarbejderne i udviklingen, samt inspiceret dokumentation.	Ingen anmærkninger
6.2	Der tilpasses og kontrolleres løbende kapaciteter i forhold til opretholdelse af driften.	Foretaget interview med medarbejder omkring rutiner for skalering af kapacitet.	Ingen anmærkninger
6.3	Løbende password-skift på både interne og eksterne systemer.	Inspiceret konfiguration for password politikker, herunder frekvens for skift at password.	Ingen anmærkninger
6.4	Logning af afviste log-on forsøg med automatisk alarmering	Inspiceret log for egenkontrol af logning af afviste login-forsøg	Ingen anmærkninger