GDPR it-sikkerhedstjekliste	Ansvar	Kategori	Dialog	Status	Påvirkning	Prioritering	Estimeret etableringstid	Estimeret tid pr. bruger
Datasikkerhed								
Adgangskontrol								
Grundlæggende								
Aktiver adgangskodepolitik (anvend min. 8 karakterer, skift hver 90. dag og forhindrer genbrug af de sidste 4 koder)		1	Ja		Mellem	1		
Anvend komplekse adgangskoder (benyt tal, specialtegn, store/små bogstaver og lås brugerkonti efter 10 forsøg i 4 timer)		2	Ja		Mellem	2		
Omdøb default administrator brugernavn		1	Nej		Lav	2		
Verficer at adgangskoder for alle konti er opsat til udløb		1	Ja		Mellem	1		
Kontroller at service konti har komplekse adgangskoder (20+ karakterer)		2	Nej		Lav	1		
Benyt ikke generiske brugernavne, såsom: sql, serviceaccount, admin osv.		1	Nej		Lav	2		
Indfør altid minimum 2 fungerende administrative konti		1	Nej		Lav	2		
Foretag årlig scanning og nedlukning af inaktive brugere og computer konti		1	Ja		Lav	2		
Tildel filadgang med særlige sikkerhedsgrupper		1	Ja		Lav	2		
Benyt et sikkert system til opbevaring af adgangskoder		2	Ja		Lav	2		
Udarbejd oversigt over hvilke medarbejder der har adgang til hvilke systemer		1	Ja		Lav	1		
Anbefalet								
Implementer 2-faktor godkendelse (Azure MFA) ekskl. licens		2	Ja		Mellem	3		
Placering								
Grundlæggende								
Bekræft at brugerdata ikke placeres på private cloud-services		1	Ja		Lav	1		
Verificer at virksomhedsdata er placeret indenfor EU		1	Ja		Lav	1		
Bekræft at alle services med kritisk brugerdata omfattes af backup		1	Ja		Lav	1		
Systemer								
Website								
Grundlæggende								
Bekræft at hjemmesidetrafik er beskyttet af et SSL-certifikat (https)		2	Ja		Lav	2		
Sørg for at adresse og betalingsoplysninger for domæne og DNS er korrekte		1	Ja		Lav	3		
Sørg for login til domæne- og DNS-administration er forsvarligt opbevaret		1	Ja		Lav	2		
Anbefalet								
Informer brugere på hjemmeside om evt. brug af cookies og privatlivspolitik		1	Ja		Lav	3		
Sørg for at have en løbende aftale om opdatering af sikkerhedsbrister i CMS-system		1	Ja		Lav	3		
Sørg for at hjemmeside-formularer ikke sender ukrypterede personfølsomme oplysninger via e-mail		1	Ja		Lav	2		
E-mail								
Grundlæggende								
Aktiver spamfilter med malware beskyttelse (ekstern scanning før truslen når ind på netværket)		1	Ja		Lav	1		
Opsæt SPF record til beskyttelse mod forfalskning		1	Ja		Lav	2		
Begræns SMTP relay med krav om login og/eller IP-begrænsning		1	Nej		Lav	2		
Anbefalet								
Office 365 – aktiver Legal Hold for følsomme postkasser		2	Ja		Lav	3		
Implementer 2-faktor godkendelse (Azure MFA) ekskl. licens		2	Ja		Mellem	2		
Opsætning af DMARC record til beskyttelse mod forfalskning		2	Ja		Lav	3		
Ekstra								
Office 365 - advar og krypter e-mails indholdende følsom data (Azure Information Protection) ekskl. licens		2	Ja		Mellem	3		
Anvend Sikkermail via NemID		2	Ja		Mellem	3		
Office 365, Advanced threat protection - beskyt post for mistænkelig aktivitet og links		3	Ja		Mellem	3		
Office 365, Data Loss Prevention - Opsæt politikker så følsomme oplysninger ikke bliver spredt via mail		3	Ja		Mellem	3		

Egenudviklede systemer								
Grundlæggende								
Bekræft at systemet er omfattet af backup		1	Ja		Lav	1		
Anbefalet								
Bekræft at data ikke er lagres ukrypteret		2	Ja		Lav	2		
Bekræft at der kan være mulighed for individuelle brugerrettigeder på dataniveau		2	Ja		Lav	2		
Sørg for at adgang til personoplysninger logges		2	Ja		Lav	1		
Sørg for at data krypteres når den overføres		2	Ja		Lav	2		
Brugerudstyr								
Computere								
Grundlæggende								
Beskyt alle computere med central styret antivirus		1	Nej		Lav	1		
Sørg for alle computere har support-agent installeret til dokumentation		1	Nej		Lav	1		
Aktiver software-firewall på alle computere		1	Nej		Lav	3		
Aktiver fast rutine for patch management		1	Ja		Mellem	2		
Sørg for operativsystem og applikationer er supporteret af leverandøren		1	Ja		Lav	2		
Sørg for at udstyret er omfattet af garanti og firmware opdatering		1	Ja		Lav	3		
Sørg for at udstyret beskyttes med adgangskode		1	Ja		Lav	1		
Anbefalet								
Begræns administrativ adgang for brugerne til deres enheder		2	Ja		Høj	3		
Opdater løbende tredjepartssoftware		1	Ja		Mellem	2		
Krypter af drev på virksomhedens computere (BitLocker)		2	Ja		Mellem	1		
Afklar om kryptering af virksomhedens computere skal på installations-tjekliste for nye computere		2	Ja		Lav	1		
Aktiver Remote Secure Erase via BIOS		3	Ja		Lav	3		
Indsaml og fjern løbende uønsket software		2	Ja		Mellem	3		
Backup af klienter ekskl. dataforbrug		2	Ja		Mellem	2		
Automatisk låsning af computere efter 10 minutters inaktivitet		2	Ja		Mellem	2		
Ekstra								
Anvend en løsning til kun afvikling af godkendte applikationer		3	Ja		Høj	3		
Mobile enheder								
Anbefalet								
Beskyt virksomhedsdata med kryptering		3	Ja		Lav	3		
Opsæt virksomhedspolitik for PIN-kode beskyttelse		2	Ja		Mellem	1		
Aktiver remote wipe funktionalitet		2	Ja		Lav	2		
Sørg for mobile enheder er opdateret		1	Ja		Mellem	3		
Indfør politik for valg af tilladte typer mobile enheder		2	Ja		Mellem	3		
Beskyt mobile enheder med antivirus ekskl. licens		3	Ja		Mellem	3		
Anvend Mobile Device Management løsning		2	Ja		Mellem	2		
Ejerskab								
Anbefalet								
Sørg for at virksomhedens enheder tilbageleveres efter brug og renses		1	Ja		Mellem	1		
Udarbejd oversigt over alle enheder internt		2	Ja		Mellem	2		
Infrastruktur								
Windows servere								
Grundlæggende								
Foretag følgende backup (daglig filbackup og image-backup - begge med overvågning)		1	Ja		Lav	1		
Beskyt alle Winsows servere med centralt styret antivirus		1	Nej		Lav	1		
Sørg for alle servere har "Supporters" agent installeret		1	Nej		Lav	1		

Aktiver fast rutine for patch management		1	Ja		Mellem	1		
Etabler overvågning af kritiske services (løbende kontrol af fejlede login forsøg)		1	Ja		Lav	2		
Aktiver Windows firewall på domæne, privat og offentlig zone		2	Ja		Lav	2		
Kontrol at default lokal administrator konto er deaktiveret		1	Nej		Lav	3		
Sørg for at 3. partsleverandører har begrænset brugeradgang		1	Ja		Lav	2		
Opsæt RDP script til blokering af IP-adresser med mange fejlede loginforsøg		1	Nej		Mellem	3		
Aktiver Volume Shadow Copy på alle netværksdrev		1	Nej		Lav	2		
Sørg for operativsystem og applikationer er supporteret af leverandøren		1	Ja		Lav	2		
Sørg for at udstyret er omfattet af garanti og firmware opdatering		1	Ja		Lav	3		
Anbefalet								
Kontroller alle relevante enheder benytter et gyldigt SSL-certifikat		2	Ja		Lav	3		
Opdater løbende forretningsspecifikke applikationer (applikationer leveret af 3. parts leverandører)		1	Ja		Lav	3		
Begræns brugernes filadgang til et minimum		2	Ja		Mellem	3		
Opret dedikerede servere til tredjepartsleverandører		2	Ja		Lav	3		
Ekstra								
Opsætning af Canarytokens		3	Ja		Lav	3		
Netværk								
Grundlæggende								
Benyt Secure DNS til eksterne opslag		1	Nej		Lav	1		
Skift generiske brugernavne (admin, user etc.)		1	Nej		Lav	2		
Anvend komplekse og unikke passwords på enheder		1	Nej		Lav	1		
Årligt skift af passwords på netværksenhder		2	Nej		Lav	3		
Opgrader årligt firmware på netværksenheder		2	Ja		Lav	3		
Foretag årligt portscanning på offentlige IP-adresser og luk unødvendige porte		2	Ja		Lav	2		
Skift årligt Wi-Fi passwords (både internt og på gæstenetværk)		2	Ja		Mellem	2		
Verificer at Wi-Fi gæstenetværket er isoleret		1	Nej		Lav	1		
Gennemgå årligt firewall for fejl og uhensigtsmæssig konfiguration		1	Nej		Lav	3		
Anbefalet								
Benyt SSL VPN til brugere (nødvendig trafik ved VPN fra private enheder)		2	Ja		Mellem	2		
Benyt L2TP som alternativ for enheder som ikke understøtter SSL VPN		2	Ja		Mellem	2		
Benyt AES og SHA kryptering til site-2-site VPN-forbindelser		2	Nej		Lav	3		
Segmenter netværkene for adskillelse af brugere og servere		3	Ja		Mellem	3		
Indfør DMZ-zone for internettilgængelige servere		2	Ja		Mellem	3		
Anvend gateway malware scanning og intrusion protection ekskl. hardware		3	Nej		Mellem	3		
Begræns offentlige IP-adresser til remote administration		1	Nej		Lav	2		
Web Application Firewall som Cloudflare eller lignende til webservere		3	Ja		Lav	3		
Ekstra								
Udfør penetrationstest på offentlige IP-adresser, mailservere og websites etc.		2	Ja		Lav	3		
Fysisk sikkerhed								
Grundlæggende								
Verficer at servere og netværksudstyr står i et aflåst rum med begrænset adgang		2	Ja		Lav	2		
Verficer at backup opbevares separat fra serverne		1	Nej		Lav	1		
Anbefalet								
Anvend privacy filtre på skærme ved arbejde med følsom data		3	Ja		Mellem	3		
Anvend elektronisk dørlås til serverrum		3	Ja		Mellem	3		
Verificer at overvågningsudstyr opbevares utilgængeligt for uvedkommende		2	Ja		Lav	3		

Printere								
Anbefalet								
Opsætning af PIN-kode på printere til beskyttet udskrivning af følsomme dokumenter		2	Ja		Mellem	3		
Politikker								
It-politik								
Grundlæggende								
Udarbejd en brugerrelateret it-politik (template kan tilsendes)		2	Ja		Mellem	2		
Udarbejd en operationel it-politik (template kan tilsendes)		2	Ja		Mellem	2		
Afklar virksomhedens politik for adgang til data hjemmefra		2	Ja		Mellem	2		
Indhent databehandler-aftaler fra systemleverandører		1	Ja		Lav	1		
Afklar overordnet krav til tilbageholdelsestid for backup		1	Ja		Lav	1		
Anbefalet								
Udarbejd datapolitik som beskriver behandling af personoplysninger		2	Ja		Høj	1		
Udarbejd systempolitik som beskriver hvordan systemerne bør anvendes		2	Ja		Lav	3		
Udarbejd oversigt over godkendte programmer		2	Ja		Mellem	2		
Ansvarfordeling (snitflader)								
Anbefalet								
Udarbejd en oversigt over systemejere		2	Ja		Lav	2		
Udarbejd en snitfladeoversigt mellem leverandører		2	Ja		Lav	2		
Afklar overordnet beslutningskompentencer vedr. rollefordeling internt		1	Ja		Lav	2		
Processer								
Compliance								
Grundlæggende								
Indfør fast procedure for eskalering af rettigheder		1	Ja		Lav	1		
Indfør fast proces for oprettelse og nedlæggelse af brugere		1	Ja		Lav	1		
Udarbejd beredskabsplan for genetablering ved systemnedbrud		2	Ja		Lav	3		
Udfør løbende stikprøvekontrol fra backup		1	Nej		Lav	1		
Revider og tilpas årligt firewallregler		2	Nej		Lav	2		
Udarbejd dokumentation over it-infrastruktur		1	Ja		Lav	1		
Revider og tilpas årligt brugernes systemadgang		2	Ja		Lav	3		
Udarbejd proces for advisering af Datatilsynet ved sikkerhedsbrist		2	Ja		Lav	2		
Governance								
Grundlæggende								
Undersøg og tag stilling til om I er/skal omfattes af en cyper og/eller dataforsikring		1	Ja		Lav	1		
Indfør årlig revidering af it- og data-politik (hent godkendelse hos Supporters ved ændringer)		2	Ja		Lav	3		
Indfør årlig revidering af processer til behandling af personoplysninger		2	Ja		Lav	3		
Anbefalet								
Logfør hændelser fra systemer der opbevarer eller overfører personoplysninger		2	Ja		Lav	3		
Logfør hændelser for gruppepolitikker		2	Nej		Lav	2		
Logfør hændelser for brugerlogins på servere		1	Nej		Lav	2		
Logfør hændelser på følsomme filplaceringer		2	Ja		Lav	2		
Logfør hændelser på følsomme postkasser		2	Ja		Lav	2		
Logfør hændelser for ændringer på administrative konti		1	Nej		Lav	2		
Uddannelse								
Brugeradfærd								
Anbefalet								
Informer om risici og sikkerhedstips		1	Nej		Lav	2		
Awareness træning for brugerne i organisationen		2	Nej		Mellem	3		