GDPR – General Data Protection Regulation (Persondataforordningen)

Første fælles "EU-lov". Gældende fra, den 25. maj 2018.

Regulering af personoplysninger i EU - også effektiv for virksomheder og organisationer, der er etableret udenfor, men som driver forretning i EU. Inkluderer al personale-, kunde- og anden personrelateret information og tilhørende data, dokumenter mv.

GDPR-politikken skal følges over hele verden, hvad angår information, kommende fra EU lande. Denne politik og tilsvarende procedurer er implementeret.

Hvad opbevarer EXIT Partners og hvad er omfattet?
Personoplysninger og data af enhver art, herunder enkeltstående, som dele af kontrakter, aftaler, lønoplysninger, oplysninger fra offentlige myndigheder mv. Det vurderes i hvert tilfælde, om der er behov for GDPR følsom viden, samt om der er lovhjemmel til indhentelse af de pågældende oplysninger, eksempelvis i forbindelse med Hvidvaskloven.

Hvordan opbevarer EXIT Partners – sikkerhed?
Data opbevares på vores servere, eller som fysiske dokumenter i mapper i aflåste skabe. Pc'er lukkes før de forlades og fysiske dokumenter medbringes eller låses inde.

Hvor længe opbevarer vi?
Oplysninger opbevares ikke længere end nødvendigt (typisk fem hele år fra forretningsomfangets afslutning) og slettes efter den nødvendige opbevaringsperiode.

Hvem har tilgang?
Adgangsbegrænsning med tilgang alene for relevante personer/ ledere. Ledelsen registrerer og administrerer, hvem der har adgang.

Hvordan håndterer EXIT Partners GDPR følsomt materiale, sendt mellem GDPR omfattede- og ikke GDPR omfattede lande?

- Så vidt muligt adskilles grænseoverskridende håndtering af GDPR følsom viden. I nødvendige tilfælde indestår modtageren for, at fortrolighed jf. GDPR tillige gælder modtageren og andre (begrænses), modtageren i en given proces/ sagsbehandling måtte finde nødvendige, at dele oplysningerne med. Modtageren delagtiggør disse i nærværende HR GDPR policy.
- Hvis personer spørger om GDPR følsomt materiale – udleveres dette ikke umiddelbart, men der henvises til leder/ ansvarlig, som vil vurdere og håndtere forespørgslen.

Fortrolighedserklæringer
I mange tilfælde benytter EXIT Partners sig af særlige fortrolighedserklæringer, der ligeledes fastlægger procedurer og sikkerhedstiltag, som sletning og ansvar.

Hvordan slettes?
Sletning skal foregå, så genskabelse af data ikke umiddelbart er muligt. Fysiske dokumenter skal makuleres, så de ikke umiddelbart kan tilvejebringes eller genskabes.

Hvordan sikrer EXIT Partners, at der slettes?
Den ansvarlige leder gennemgår følsomt materiale en gang årligt med henblik på sletning af overflødige oplysninger.

Hvad gør EXIT Partners ved mistanke om sikkerhedsbrist?
Mistanke skal omgående rapporteres til nærmeste ansvarlige, eller foresatte.

Hvad gøre EXIT Partners ved konstateret sikkerhedsbrist?
- Data sikres på optimal vis.
- Eventuelt overflødige data slettes på forsvarlig vis.
- Brugere orienteres og det sikres, at deres viden er opdateret.
- Procedurer gennemgås og eventuelle ændringer implementeres og oplyses.

TK/ 15.09.2018

Med venlig hilsen

Torben Kristensen