

Politik		Persondata GDPR	
Udarbejdet af:	Version:	Dato:	Side:
Bestyrelsen/AVA	3.0	30/7 2019	Side 1 af 2

Indledning

Den 25. maj 2018 trådte EU's persondataforordning med navnet General Data Protection Regulation (GDPR) i kraft i hele EU. Derefter skal virksomheder, offentlige myndigheder og organisationer, der behandler persondata opfylde den nye forordning. GDPR (plus ny national lovgivning) afløser den nuværende persondatalov. EU-forordning har direkte lovlig gyldighed i modsætning til et EU-direktiv, som skal implementeres via national lovgivning.

Formålet

GDPR har som formål at styrke og ensrette databeskyttelsen for individer i EU. Det primære mål med GDPR er at beskytte data, sikre borgerne kontrol over egne persondata og forenkle lovgivningen vedrørende international handel, ved at ensrette love og regelsæt inden for EU. GDPR pålægger organisationer at beskytte persondata via organisatoriske, administrative og tekniske tiltag og denne beskyttelse skal dokumenteres. GDPR udstikker strenge krav til samtykke og transparens (gennemsigtighed). For at opfylde kravene skal organisationer, der bruger persondata om individer, indhente personernes udtrykkelige samtykke.

Hvilke data kommer NærBrand i besiddelse af – og hvordan?

Fra vores samarbejdspartner Topdanmark modtager vi løbende oplysninger indeholdende:

- 1) Unikt, af Topdanmark tildelt, kundenummer pr. person eller virksomhed, der knyttes til:
 - a) Navn, adresse, telefonnummer og e-mailadresse.
 - b) Tilhørende policetype og policenummer
 - c) Policernes brandpræmie, præmieandel, selvrisiko og tilhørende risikosum
 - d) Afholdte og forventede skadesudgifter pr. police.

Der modtages således ingen personfølsomme personoplysninger, ej heller cpr. nummer i forbindelse med udveksling af kundeportefølje

De modtagne oplysninger er i sagens natur personhenførbare, således at et datalæk vil kunne afsløre hvem NærBrand har som medlemmer/kunder. Disse oplysninger opbevares på NærBrands krypterede PC, samt på Bestyrelsesportalen BetterBoard, hvorfra det kan downloades og printes af alle bestyrelsesmedlemmer.

I forbindelse med skadesoplysninger kan forekomme personfølsomme oplysninger, idet disse oplysninger søges af NærBrand direkte i Topdanmarks it-systemer, og kan dataoverføres til NærBrands systemer. Disse data opbevares således alene på NærBrands krypterede PC.

I forbindelse med medlemmernes mulighed for at købe sikkerhedsudstyr modtager NærBrand selv, via hjemmesiden/e-mail, samme almindelige navneoplysninger. NærBrand videregiver alene disse oplysninger når en 3. part skal forestå levering.

Hvad gør NærBrand

Bestyrelsen ønsker, at dens medlemmers oplysninger, og oplysninger i forbindelse med potentielle kundeforhold bliver behandlet efter forordningen. Bestyrelsen ønsker at direktøren har størst mulig opmærksomhed på muligt databrud, og omgående reagerer såfremt det konstateres.

Bestyrelsen pålægger sig selv (sine medlemmer), at undlade at downloade eller udskrive disse bilag.

Såfremt bestyrelsesmedlemmet vælger det alligevel skal de ske med forsigtighed, og bilagene skal omhyggeligt slettes/destrueres efter endt læsning/behandling.

Sådan forholder NærBrand sig:

1. Databeskyttelsespolitik i forhold til medarbejderne – dvs. oplysningspligten overfor medarbejdere om, hvilke data om dem der behandles:
 - ⇒ Alle modtagere af honorarer fra NærBrand har afgivet yderligere oplysninger og har alle tiltrådt behandlingen af dem på en erklæring som bilag 1 nedenfor.
2. Privatlivs "politik" på webside – den generelle oplysningsforpligtelse overfor kunder og eksterne parter
 - ⇒ NærBrand har skiftet leverandør i 2019, og den nye leverandør sikrer opfyldelse.
3. Retningslinjer og instrukser om slettestrifter.
 - ⇒ Den personhenførbare del af kundeoplysningerne bliver slettet efter 3 år. De tilbageværende oplysninger anvendes til statistik.
 - ⇒ Fristen på 3 år sættes med henvisning til forsikringsaftalelovens §29 om frist for efteranmeldelse af skader.
 - ⇒ NærBrand sletter de indhentede oplysninger om specifikke skader når de er 10 år gamle. Fristen sættes som en konsekvens af kundens ret til at genoptage afsluttede sager.

Politik		Persondata GDPR	
Udarbejdet af:	Version:	Dato:	Side:
Bestyrelsen/AVA	3.0	30/7 2019	Side 2 af 2

4. Procedure til besvarelse af henvendelser om de registreredes rettigheder; indsigt, ajourføring, dataportabilitet mv. ses således ikke særlig påtrængende hos NærBrand. Vi forholder os til:
 - a. Retten til at modtage oplysning om en behandling af sine personoplysninger (oplysningspligt).
 - ⇒ Håndteres af Topdanmark ved indsamling af oplysningerne.
 - b. Retten til at få indsigt i sine personoplysninger (indsigtsret).
 - ⇒ Kan umiddelbart imødekommes af direktøren.
 - c. Retten til at få urigtige personoplysninger berigtiget (retten til berigtigelse)
 - ⇒ Kan umiddelbart imødekommes af direktøren.
 - d. Retten til at få sine personoplysninger slettet (retten til at blive glemt)
 - ⇒ Kan umiddelbart imødekommes af direktøren.
 - e. Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring
 - ⇒ NærBrand bruger ikke personoplysninger i sin markedsføring.
 - f. Retten til at flytte sine personoplysninger (dataportabilitet)
 - ⇒ Kan umiddelbart imødekommes af direktøren.
5. Retningslinjer/instruks i tilfælde af inspektion/kontrolbesøg.
 - ⇒ I tilfælde af inspektion vil NærBrands samlede datamængde, af direktør Martin Damholdt, blive stillet til rådighed for inspektionen.
6. NærBrand udnævner direktør Martin Damholdt til selskabets Databeskyttelsesrådgiver.

Vedtaget på bestyrelsesmødet 30. juli 2019
 Karsten Bak Poulsen, mødeleder