

## **Privatlivspolitik.**

### **1. Navn og kontaktoplysninger**

Reform-Gruppen ApS er dataansvarlig, og dette dokument indeholder en fortegnelse over alle kategorier af behandlingsaktiviteter, som udøves under virksomhedens ansvar.

Kontaktoplysninger:

Reform-Gruppen ApS  
CVR-nr. 36919329  
Adelvej 80  
7000 Fredericia  
E-mail: info@reform-Gruppen.dk  
Kontaktperson: Johnny A. Paaskesen  
Telefonnummer: 70267686

### **2. Formål med behandling**

Reform-Gruppen ApS behandler personoplysninger med henblik på:  
Formidling af boligkreditaftaler samt udbud af dennes muligheder.

### **3. Kategorier af registrerede personer**

Der behandles oplysninger om følgende kategorier af registrerede personer og eller selskaber.

1. Låneansøgere for boligkreditformidling

### **4. Kategorier af personoplysninger**

Følgende kategorier af almindelige personoplysninger indgår i den specifikke behandling af de registrerede personer og eller selskaber.

1. Identifikations- og kontaktoplysninger – Låneansøgere
2. Identifikations- og kontaktoplysninger – Boligkreditformidlere, herunder banker samt sparekasser.
3. Identifikations- og kontaktoplysninger – Leverandører

Reform-Gruppen ApS indsamler og behandler følsomme personoplysninger.

Reform – Gruppen ApS indsamler eller behandler ikke oplysninger om strafbare forhold.

## **5. Modtagere af personoplysninger i EU**

Reform-Gruppen ApS videregiver personoplysningerne til følgende samarbejdspartnere/databehandlere:<sup>1</sup>

1. Danske banker og sparekasser.
2. Godkendte af finansstilsynet boligkreditformidlere / ejendomskreditselskaber
3. Dropbox Erhverv
4. Offentlige myndigheder – eksempelvis SKAT

## **6. Modtagere af personoplysninger i tredjelande eller internationale organisationer**

Reform-Gruppen ApS overfører ikke personoplysninger til databehandlere i tredjelande uden for EU eller til internationale organisationer.

## **7. Sletning af oplysninger**

Reform- Gruppen ApS sletter/returnerer personoplysninger efter følgende regler:

1. Ved førtidsindfrielse af udbudte boligkredit / boliglån
2. Ved endt løbetid
3. ved ikke godkendt boligkreditaftale dog max 12 mdr.

Samtlige ovennævnte frister for sletning kan konkret fraviges, såfremt der er en saglig begrundelse herfor, herunder eksempelvis verserende retssag med den registrerede som part.

Sletning foregår manuelt.

## **8. Tekniske og organisatoriske sikkerhedsforanstaltninger**

Ved blandt andet design og databeskyttelse gennem standardindstillinger træffer reform-Gruppen ApS de fornødne tekniske og organisatoriske foranstaltninger, som måtte være nødvendige for at sikre, at personoplysningerne ikke hændeligt eller ulovligt tilintetgøres, offentliggøres, bliver brugt til andet end formålet, fortabes, ændres eller bliver misbrugt af uvedkommende mv. Til sikring af foranstående fortager Foreningen følgende tekniske og organisatoriske foranstaltninger:

1. Reform-Gruppen ApS opbevarer alle personoplysninger på virksomhedens computer, som er beskyttet af en firewall og antivirussoftware samt låst inde, og som er beskyttet af koder. Alene reform-Gruppen ApS og dennes medarbejdere kender koderne.
2. Etablerer og vedligeholder log-in og adgangskodeprocedure til it-systemer, herunder servere, samt opsætter en firewall og antivirussoftware mv. til sikring af vedvarende fortrolighed, integritet og robusthed af it-systemerne.
3. Der anvendes personlige koder for at få adgang til pc'ere.
4. Sikrer at eventuelle papirformater mv. indeholdende personoplysninger behandles og opbevares efter samme regler som gældende for elektroniske formater samt sikkerhedsmakuleres og –destrueres.
5. Tilrettelægger tekniske og organisatoriske foranstaltninger til sikring af, at alene virksomheden og dennes medarbejdere med saglige formål har adgang til personoplysningerne, og at disse er bekendte og ajourførte med de etablerede sikkerhedsforanstaltninger og relevante regler for behandling af personoplysningerne.
6. Sikrer at de personer, der er autoriseret til at behandle personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt lovbestemt tavshedspligt.
7. Sikrer procedurer til genoprettelse af tilgængeligheden af og adgang til personoplysningerne i tilfælde af en fysisk eller teknisk utilsigtet hændelse.
8. Etablerer en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de i pkt. 1 til 7 foranstaltninger.

## 9. Brud på persondatasikkerheden

Ved brud på persondatasikkerheden forstås et brud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er behandlet. Ved alle brud vil der manuelt blive forsøgt begrænsning af skaden og genoprettelse hurtigst muligt.

Såfremt et brud medfører en risiko for fysiske personers rettigheder og frihedsrettigheder – hvilket blandt andet omfatter risiko for diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede – sker der anmeldelse til Datatilsynet uden unødigt forsinkelse og om muligt senest 72 timer efter, at man er blevet bekendt med bruddet.

Ved risikovurderingen vil følgende momenter blive inddraget:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse
- Oplysningernes art og omfang
- Risikoen for at registrerede kan identificeres
- Konsekvenser bruddet kan have for de registrerede
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. hvis der er tale om børn eller særligt udsatte)
- Antallet af berørte fysiske personer

Anmeldelse vil blive foretaget af kontaktpersonen, jf. pkt. 1.

Hvis et brud indebærer en høj risiko for fysiske personers rettigheder og frihedsrettigheder, vil de berørte registrerede uden unødigt forsinkelse blive direkte underrettet om bruddet. Underretning vil ske via e-mail, brev, sms eller lignende.

Hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, foretages der ikke anmeldelse til Datatilsynet eller den registrerede.

Ved brud, der skal anmeldes, sker indberetning til myndighederne via Datatilsynets digitale indberetningsløsning på virk.dk.

Uanset om et brud anmeldes eller ej, vil virksomheden i tilfælde af brud udarbejde en skriftlig redegørelse for bruddet, som minimum vil indeholde følgende punkter:

- Dato og tidspunkt for bruddet
- Hvad skete der i forbindelse med bruddet?
- Hvad er årsagen til bruddet?
- Hvilke (typer) personoplysninger er omfattet af bruddet?
- Hvilke konsekvenser har bruddet for de berørte personer?
- Hvilke afhjælpende foranstaltninger er truffet?
- Hvorvidt der er sket anmeldelse til Datatilsynet eller ej?

## **10.Øvrige oplysninger**

Denne fortegnelse foreligger såvel skriftligt som elektronisk.

Udarbejdet maj 2018