

Sådan beregnes...

GDPR- BØDER

På GDPR-området lægges der med Databeskyttelsesforordningen op til et nyt, væsentligt højere bødeniveau, der gennem retspraksis skal skabe grundlag for mere ensartede, gennemskuelige og til dels standardiserede bøder for konkrete overtrædelser af de databeskyttelsesretlige regler.

Derfor har Datatilsynet udarbejdet en vejledning til, hvordan de konkrete bødestørrelser fastsættes. I dette White Paper har vi prøvet at koge den officielle vejledning ned til en lækker lille bouillon-terning.

Beregningsmodel for bøder

Helt overordnet skal en bøde...

- ▶ være *effektiv*
- ▶ stå i rimeligt *forhold* til overtrædelser
- ▶ have *afskrækkende* virkning

Grundlæggende baseres bøden på et grundbeløb, der efterfølgende justeres efter virksomhedens størrelse samt overtrædelsens karakter, alvor og varighed.

Dernæst vurderes det, om der er skærpende eller formildende omstændigheder, og endelig tilrettes bøden blandt andet efter betalingsevne. Regnestykket ser altså således ud:

Grundbeløb

- +/- justering efter overtrædelsens karakter, alvor og varighed
- + skærpende omstændigheder
- formildende omstændigheder

Justeret grundbeløb

- evt. justering efter databeskyttelsesforordningens maksimum
- evt. justering efter betalingsevne

Endeligt bødebeløb

Grundbeløbet

Grundbeløbet tager udgangspunkt i store virksomheder med en omsætning op til 500 mill. kr.

Men beløbet justeres efter virksomhedens størrelse alt efter, om man er en mellemstor (< 375 mill. kr.), lille (< 75 mill. kr.) eller mikro-virksomhed (< 15 mill. kr.).

Da bøden både skal være effektiv, forholdsmæssig og afskrækkende, inddeles overtrædelserne desuden i kategorier efter grad af alvorlighed.

Justering efter overtrædelsens karakter, alvor og varighed

Efter at have fastlagt grundbeløbet, justeres bøden efter overtrædelsens karakter, alvor og varighed i det konkrete tilfælde, hvilket omfatter...

Behandlingens omfang

Udføres behandlingen lokalt, nationalt eller grænseoverskridende?

Formål med behandlingen

Er formålet anerkendelsesværdigt?

– i givet fald bedømmes det mildere.

Antal registrerede

Hvor mange registrerede er egentligt berørt

– og hvor mange kunne potentielt blive berørt?

Omfanget af den skade, der er lidt

Hvilken og hvor alvorlig er den skade, de berørte registrerede har lidt?

Varighed

Hvor længe har overtrædelsen stået på?

– jo længere, desto højere straf.

Skærpende og formildende omstændigheder

Dernæst kan der ske en stigning af beløbet ved skærpende omstændigheder og/eller et fald ved formildende omstændigheder. Det drejer sig om...

- ▶ blev overtrædelsen begået forsættligt eller uagtsomt?
- ▶ hvilke foranstaltninger er der truffet for at begrænse skaden?
- ▶ hvor vidt der er gennemført passende tekniske og organisatoriske sikkerhedsforanstaltninger?
- ▶ er der relevante tidligere overtrædelser?
- ▶ graden af samarbejde med tilsynsmyndigheden for at afhjælpe overtrædelsen og begrænse de negative konsekvenser af overtrædelsen?
- ▶ hvilke kategorier af personoplysninger er berørt af overtrædelsen?
- ▶ hvordan og hvor meget er tilsynsmyndigheden blevet gjort bekendt med overtrædelsen?
- ▶ er der truffet tidligere lignende foranstaltninger over for den pågældende virksomhed?
- ▶ er alle godkendte adfærdskodekser eller godkendte certificeringsmekanismer overholdt?
- ▶ er der andre skærpende eller formildende faktorer ved sagens omstændigheder?

Justering efter databeskyttelsesforordningens maksimum

Hvis bøden overstiger maksimum fastsat i databeskyttelsesforordningen, skal bødes justeres. Der er fastsat et statisk og et dynamisk bødeloft, der igen afhænger af graden af alvorlighed.

Det statiske bødeloft går op til 75 mill. kr. (€ 10 mill.) ifølge artikel 83, stk. 4, mens loftet er 150 mill. kr. (€ 20 mill.) for artikel 83, stk. 5.

Det dynamiske bødeloft er henholdsvis 2% eller 4% af virksomhedens samlede globale årlige omsætning i det foregående regnskabsår.

Bødeloftet fastsættes efter hvilket beløb, der er størst – det statiske eller det dynamiske.

Justering efter betalingsevne

Bøden skal som nævnt matche overtrædelsens karakter, alvor og varighed, så hvis en høj bøde medfører konkurs, bør det altid overvejes, om målet kan nås med en mindre bøde. Det kan godt være, at en sådan bøde er både effektiv og afskrækkende, men den skal også være proportional.

Derfor kan bøden i særlige tilfælde nedsættes grundet manglende betalingsevne – eller alternativt udsættes. Men det kræver ekstraordinære omstændigheder, og nedsættelse kan kun ske, hvis der foreligger objektive beviser for, at den pålagte bøde med sikkerhed vil bringe den pågældende virksomheds økonomiske levedygtighed i fare.

Artikel 83, stk. 4 (*overtrædelse af forpligtelser*)

Overtrædelse af følgende bestemmelser straffes i overensstemmelse med stk. 2 med administrative bøder på op til € 10.000.000, eller hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere:

- a den dataansvarliges og databehandlerens forpligtelser i henhold til art. 8, 11, 25-39 og 42 og 43
- b certificeringsorganets forpligtelser i henhold til art. 42 og 43
- c kontrolorganets forpligtelser i henhold til art. 41, stk. 4. 4.5.2016 L 119/82 Den Europæiske Unions Tidende DA

Artikel 83, stk. 5 (*overtrædelse af grundlæggende principper*)

Overtrædelse af følgende bestemmelser straffes i overensstemmelse med stk. 2 med administrative bøder på op til € 20.000.000, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere:

- a de grundlæggende principper for behandling, herunder betingelserne for samtykke, i art. 5, 6, 7 og 9
- b de registreredes rettigheder i henhold til art. 12-22
- c overførsel af personoplysninger til en modtager i 3. land eller en int. organisation i henh. til art. 44-49
- d eventuelle forpligtigelser i medfør af medlemsstaternes nationale ret vedtaget i henhold til kapitel IX
- e manglende overholdelse af et påbud eller en midlertidig eller definitiv begrænsning af behandling eller tilsynsmyndighedens suspension af overførsel af oplysninger i henhold til art. 58, stk. 2, eller manglende adgang i strid med art. 58, stk. 1.

Overtrædelse	Artikel
Databeskyttelsesforordningens artikel 83, stk. 4: Overtrædelse af forpligtelser	
· Udpegning af repræsentant	27
· Samarbejde med tilsynsmyndigheden	31
· Behandling der ikke kræver identifikation	11
· Fortegnelse over behandlingsaktiviteter	30
· Anmeldelse af brud på persondatasikkerheden	33
· Udpegning mv. af databeskyttelsesrådgiver (DPO)	37-39
· Børns samtykke	8
· Privacy by design	25
· Fælles dataansvarlige	26
· Databehandleraftale	28
· Behandling der udføres for den dataansvarlige/databehandleren	29
· Behandlingsikkerhed	32
· Underretning ved brud på persondatasikkerheden	34
· Konsekvensanalyse (DPIA)	35-36
· Kontrol med godkendte adfærdskodekser	41, stk 4
· Certificering	42-43
Databeskyttelsesforordningens artikel 83, stk. 5: Overtrædelse af grundlæggende principper	
· Underretning af modtagere ved sletning mv.	19
· Ret til dataportabilitet	20
· Grundprincipperne	5
· Samtykke	7
· Gennemsigtighed	12
· Oplysningspligten ved indsamling af personoplysninger hos den registrerede selv	13
· Lovlig behandling	6
· Oplysningspligten ved indsamling af personoplysninger hos andre end den registrerede selv	14
· Indsigtsretten	15
· Ret til berigtigelse	16
· Retten til sletning	17
· Ret til begrænsning af behandling	18
· Ret til indsigelse	21
· Automatiske individuelle afgørelser, herunder profilering	22
· Behandling af særlige kategorier af personoplysninger	09.okt
· Overførsler til tredjelande og internationale organisationer	44-49

Kategori	Grad	Grundsats % af bødeloft	Grundbeløb Oms: < 500 mill.	Mellem virks. Oms: < 375 mill. 10% af GB	Små virks. Oms: < 75 mill. 2% af GB	Mikro virks. Oms: < 15 mill. 0,4% af GB
Bødeloft: 75 mill. kr. ELLER 2% af global oms.						
1	Alvorlig	5	3.750.000	375.000	75.000	15.000
2	Mere alvorlig	10	7.500.000	750.000	150.000	30.000
3	Mest alvorlig	20	15.000.000	1.500.000	300.000	60.000
Bødeloft: 150 mill. kr. ELLER 4% af global oms.						
4	Alvorlig	5	7.500.000	750.000	150.000	30.000
5	Mere alvorlig	10	15.000.000	1.500.000	300.000	60.000
6	Mest alvorlig	20	30.000.000	3.000.000	600.000	120.000

GDPR handler om mennesker

Lexoforms ønsker at lette arbejdet med at dokumentere GDPR for små og mellemstore virksomheder på en korrekt, brugervenlig, uvildig og enkel måde.

GDPR handler nemlig om at passe på hinanden og udvise respekt de data, andre betror os.

Med vores løsning skal du kun registrere de samme data én gang. Det gør hele opgaven lidt lettere...