Databehandleravtale – Hogrefe Testsystem (HTS)

Behandling av personopplysninger

Basert på uoffisiell versjon av databehandleravtale fra Danske Datatilsynet oversatt til norsk av norske Datatilsynet. Versjon 03 21.02.2024

1. Standard Avtalevilkår

i henhold til artikkel 28 nummer 3, i Europaparlamentets og Rådets forordning 2016/679 (personvernforordningen) med henblikk på databehandlerens behandling av personopplysninger

mellom

Navn			
Org.nr.			
Adresse			
Postnummer		**By**	
Land			

heretter «den Behandlingsansvarlige»

og

Hogrefe Norge AS

Org.nr. 932 802 422

Oscars Gate 35 A

0258 Oslo

Norge

heretter «Databehandleren»

som hver for seg er en «part» og sammen utgjør «partene»

Har avtalt følgende standardavtalevilkår «Vilkårene» med henblikk på å overholde personvernforordningen og sikre beskyttelse av fysiske personers grunnleggende rettigheter og friheter.

Innhold

2. Innledning

1. Disse Vilkårene fastsetter den Behandlingsansvarlige og Databehandlerens rettigheter og plikter når Databehandleren utfører behandling av personopplysninger på vegne av den Behandlingsansvarlige.

2. Disse bestemmelsene er utformet for å sikre partenes etterlevelse av artikkel 28 tredje ledd i Europaparlamentets og rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (personvernforordningen).

3. I forbindelse med levering av Hogrefe Testsystem (HTS) behandler Databehandleren personopplysninger på vegne av den Behandlingsansvarlig i henhold til disse vilkårene.

4. Vilkårene har forrang i forhold til eventuelle tilsvarende bestemmelser i andre avtaler mellom partene.

5. Det er fire vedlegg til disse Vilkårene, og vedleggene utgjør en integrert del av Vilkårene.

6. Vedlegg A inneholder nærmere opplysninger om behandlingen av personopplysninger, herunder formålet med og arten av behandlingen, type personopplysninger som behandles, kategoriene av registrerte personopplysninger og varigheten av behandlingen.

7. Vedlegg B inneholder den Behandlingsansvarliges betingelser for Databehandlers bruk av underdatabehandlere, og liste over underdatabehandlere som den Behandlingsansvarlige har godkjent.

8. Vedlegg C inneholder den Behandlingsansvarliges instrukser når det gjelder Databehandlers behandling av personopplysninger, beskrivelse av sikkerhetstiltak databehandler som minimum skal gjennomføre, samt hvordan revisjonen av Databehandleren og eventuelle underbehandlere skal utføres.

9. Vedlegg D er en oversikt over Technical and Organizational Measures (TOM).

10. Vilkårene med tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk, av begge parter.

11. Disse Vilkårene fritar ikke Databehandleren fra plikter som Databehandleren er pålagt etter personvernforordningen eller annen lovgivning.

3. Den Behandlingsansvarliges rettigheter og plikter

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i overensstemmelse med personvernsforordningen (*se* personvernforordningen artikkel 24), gjeldende personvernbestemmelser i unionsrett eller medlemslandenes[1] nasjonale lover.

[1] Henvisning til medlemslandene i disse Vilkårene skal forstås som en henvisning til land som også er en del av det europeiske økonomiske samarbeidsområdet (EØS).

2. Den Behandlingsansvarlige har rett og plikt til å bestemme formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.
3. Den Behandlingsansvarlige har blant annet ansvar for å påse at det er et behandlingsgrunnlag for behandling av personopplysninger som Databehandler er pålagt å utføre.

4. Databehandleren handler etter instruks

1. Databehandleren kan kun behandle personopplysninger etter dokumenterte instrukser fra den Behandlingsansvarlige, med mindre annet kreves av unionsretten eller medlemsstatenes nasjonale rett som Databehandleren er underlagt. Disse instruksene skal være spesifisert i vedlegg A og C. Etterfølgende instrukser kan også gis av den Behandlingsansvarlige mens personopplysninger behandles, men instruksen skal alltid være dokumentert og oppbevares skriftlig, herunder elektronisk, sammen med disse Vilkårene.

2. Databehandleren skal omgående underrette den Behandlingsansvarlige dersom en instruks fra den Behandlingsansvarlige, etter Databehandlerens mening, er i strid med personvernforordningen eller gjeldende personopplysningsbestemmelser i unionsretten eller i medlemsstatenes nasjonale rett.

5. Konfidensialitet

1. Databehandleren kan kun gi tilgang til personopplysninger som behandles på vegne av den Behandlingsansvarlige, til personer som er underlagt Databehandlerens instruksjonsmyndighet, som har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt, og bare i den grad det er nødvendig. Listen over personer som har fått innsyn skal gjennomgås fortløpende. På bakgrunn av denne gjennomgangen kan tilgang til personopplysninger stenges dersom tilgang ikke lenger er nødvendig, og personopplysningene skal ikke lenger være tilgjengelige for disse personene.

2. Databehandler skal på forespørsel fra den Behandlingsansvarlige kunne påvise at de aktuelle personene underlagt databehandlers instruksjonsmyndighet, er underlagt ovennevnte taushetsplikt.

6. Behandlingssikkerhet

1. Personvernforordningen artikkel 32 fastslår at idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenheng den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den Behandlingsansvarlige og Databehandleren gjennomføre egnede tekniske og organisatoriske tiltak (Technical and Organziational measures (TOM)) for å oppnå et sikkerhetsnivå som er passende sett i forhold til risikoen.

   Den Behandlingsansvarlige skal vurdere risikoen for fysiske personers rettigheter og friheter som behandlingen utgjør, og gjennomføre tiltak for å imøtegå disse risikoene. Avhengig av deres relevans, kan det omfatte:

   a. Pseudonymisering og kryptering av personopplysninger (kun bruke anonym data)

b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet for behandlingssystemer og tjenester.

c. evne til raskt å gjenopprette tilgjengeligheten til og tilgangen til personopplysninger i tilfelle en fysisk eller teknisk hendelse.

d. en prosedyre for regelmessig testing, vurdering og evaluering av effektiviteten av de tekniske og organisatoriske tiltakene for å sikre behandlingssikkerhet.

2. Ifølge personvernforordningen artikkel 32 skal Databehandleren – uavhengig av den Behandlingsansvarlige – også vurdere risikoen for fysiske personers rettigheter og friheter som behandlingen medfører, og iverksette tiltak for å imøtegå disse risikoene. Den Behandlingsansvarlige må stille den nødvendige informasjonen til rådighet for Databehandleren som gjør vedkommende i stand til å identifisere og vurdere slike risikoer.

3. Databehandleren skal også bistå den Behandlingsansvarlige med å overholde den Behandlingsansvarliges plikter etter personvernforordningens artikkel 32, ved bl.a. å stille til den Behandlingsansvarliges rådighet nødvendig informasjon om de tekniske og organisatoriske sikkerhetstiltak som databehandleren allerede har gjennomført i henhold til personvernforordningen artikkel 32, samt all annen informasjon som er nødvendig for at den behandlingsansvarlige skal overholde sin plikter etter personvernforordningen artikkel 32.Dette finnes bl.a. i vedlegg D

   Hvis imøtegåelse av identifiserte risikoer – etter den behandlingsansvarliges vurdering – krever at det gjennomføres ytterligere tiltak enn de databehandler allerede har iverksatt, skal den Behandlingsansvarlig angi disse tiltakene i Vedlegg C.

7. Bruk av underdatabehandlere (underleverandører tilknyttet HTS)

1. Databehandleren skal oppfylle betingelsene som er fastsatt i personvernforordningen artikkel 28 ledd 2, og ledd 4, for å gjøre bruk av en annen databehandler (en underdatabehandler).

2. Databehandleren kan ikke benytte seg av en underdatabehandler for å oppfylle Vilkårene uten på forhånd å ha innhentet en generell skriftlig godkjennelse fra den Behandlingsansvarlige.

3. Ved signatur på denne avtalen har Databehandleren den Behandlingsansvarliges generelle godkjennelse til å benytte underdatabehandlere. Databehandleren skal skriftlig underrette den Behandlingsansvarlige om eventuelle planlagte endringer som gjelder tilføyelse eller utskiftning av underdatabehandlere med minst 30 dagers varsel, og dermed gi den behandlingsansvarlige mulighet til å motsette seg slike endringer før den eller de beskrevne underdatabehandler(e) engasjeres. Lengre varslingsfrister for spesifikke underdatabehandlertjenester kan angis i vedlegg B.

   Listen over underbehandlere som den Behandlingsansvarlige allerede har godkjent fremgår av vedlegg B.

4. Når Databehandleren engasjerer en underdatabehandler for å utføre konkrete behandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal Databehandleren gjennom kontrakt eller annet juridisk dokument pålegge underdatabehandleren de samme forpliktelsene til vern av personopplysninger som er fastsatt i disse Vilkårene. I dokumentet skal det gis tilstrekkelig garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordningen.

   Databehandler er derfor ansvarlig for å kreve at underdatabehandlere som et minimum overholder Databehandlers forpliktelser etter disse Vilkårene og etter personvernforordningen.

5. En kopi av Underdatabehandleravtale(r) og eventuelle etterfølgende endringer skal – etter anmodning fra den Behandlingsansvarlige - sendes til den Behandlingsansvarlige, som derved har mulighet til å sikre at underdatabehandleren er pålagt de samme forpliktelsene til vern av personopplysninger som følger av disse Vilkårene. Kommersielle bestemmelser som ikke påvirker det personopplysningsvernsrettslige innholdet av underdatabehandleravtalen, er ikke underlagt kravet om kopi til den Behandlingsansvarlige.

6. Databehandleren skal i underdatabehandleravtalen inkludere den Behandlingsansvarlige som begunstiget tredjepart i tilfelle Databehandleren går konkurs, slik at den Behandlingsansvarlig kan tre inn i databehandlers rettigheter mht. personvernforordningen og gjøre dem gjeldende ovenfor underdatabehandlere, hvilket for eksempel setter den Behandlingsansvarlige i stand til å instruere underdatabehandleren om å slette personopplysninger.

7. Databehandleren er ansvarlig overfor den Behandlingsansvarlige når det gjelder oppfyllelse av underdatabehandlerens forpliktelser til å verne om personopplysninger i tråd med forordningen. Dette påvirker ikke de registrertes rettigheter etter personvernforordningen – særlig de nedfestet i personvernforordningen artikkel 79 og 82 – overfor den Behandlingsansvarlige og Databehandleren, herunder underdatabehandleren.

8. Overføring til tredjeland eller internasjonale organisasjoner

1. Databehandleren kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumentert instrukser fra den Behandlingsansvarlige. Slik overføring skal alltid skje i samsvar med kapittel V i personvernforordningen.

2. Hvis overføring av personopplysninger til tredjeland eller internasjonale organisasjoner som den Behandlingsansvarlige ikke har instruert Databehandler om å gjøre, er påkrevd i henhold til Unionsretten eller medlemsstatens nasjonale rett, skal Databehandler underrette den Behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr en slik underretting.

3. Uten dokumenterte instrukser fra den Behandlingsansvarlige kan Databehandleren ikke innenfor rammen av denne forskriften:

   a. overføre personopplysninger til en Behandlingsansvarlig eller Databehandler i et tredjeland eller en internasjonal organisasjon.
   b. overlate behandlingen av personopplysninger til en underbehandler i et tredjeland.
   c. behandle personopplysningene i et tredjeland.

4. Den Behandlingsansvarliges instruks om overføring av personopplysninger til tredjeland, herunder eventuelt overføringsgrunnlag i kapittel V i personvernforordningen som overføringen bygger på, skal komme frem av vedlegg C punkt C.6.

5. Disse Vilkårene skal ikke forveksles med standard personvernbestemmelser som omhandlet i personvernforordningen artikkel 46 ledd 2 bokstav c og d, og disse Vilkårene kan ikke utgjøre et grunnlag for overføring av personopplysninger under personvernforordningen kapittel V.

9. Bistand til den Behandlingsansvarlige

1. Databehandleren bistår den Behandlingsansvarlige så langt det er mulig ved hjelp av hensiktsmessige tekniske og organisatoriske tiltak (TOM) med oppfyllelse av den Behandlingsansvarliges plikt til å svare på forespørsler om utøvelse av den registrertes rettigheter som fastsatt i personvernsforordningen kapittel III.

   Dette innebærer at Databehandler så langt det er mulig skal bistå den Behandlingsansvarlig i den Behandlingsansvarliges oppfyllelse av:

   a. opplysningsplikt ved innsamling av personopplysninger fra den registrerte
   b. opplysningsplikt dersom personopplysninger ikke innhentes fra den registrerte
   c. innsynsretten
   d. rett til retting
   e. retten til sletting («retten til å bli glemt»)
   f. rett til å begrense behandlingen
   g. underretningsplikten i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
   h. retten til dataportabilitet
   i. retten til å protestere
   j. rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisk behandling, herunder profilering.

2. I tillegg til Databehandlers forpliktelse til å bistå den Behandlingsansvarlige i henhold til Vilkårene 6.3, bistår Databehandler også, med hensyn til behandlingens art og informasjonen som er tilgjengelig for Databehandleren, den Behandlingsansvarlige med:

   a. den Behandlingsansvarliges forpliktelse til å rapportere brudd på personopplysningssikkerheten til vedkommende tilsynsmyndighet, Datatilsynet, uten ugrunnet opphold og om mulig senest 72 timer etter at han har fått kjennskap til det, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og frihet.
   b. den Behandlingsansvarliges forpliktelse til å varsle den registrerte, uten ugrunnet opphold, om brudd på personopplysningssikkerheten, når det er sannsynlig at bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter
   c. den Behandlingsansvarliges forpliktelse til før behandling å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (en konsekvensanalyse).

   d. den Behandlingsansvarliges forpliktelse til å rådføres seg med den kompetente tilsynsmyndigheten, Datatilsynet, før behandlingen, dersom en konsekvensanalyse tilsier at behandlingen vil medføre en høy risiko og dersom den Behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

3. Partene skal i vedlegg C angi de nødvendige tekniske og organisatoriske tiltak som Databehandleren skal bistå den Behandlingsansvarlige med, samt omfang og utstrekning av bistand. Dette gjelder forpliktelsene som følger av Vilkårene punkt 9.1. og 9.2.

10. Melding om brudd på personopplysningssikkerheten

1. Ved brudd på personopplysningssikkerheten skal Databehandleren, uten ugrunnet opphold etter å ha blitt kjent med at det har skjedd et brudd på personopplysningssikkerheten, underrette den Behandlingsansvarlige.

2. Databehandlers underretning til den Behandlingsansvarlige skal om mulig skje senest 36 timer etter at behandlingsansvarlig har fått kjennskap til bruddet, slik at den Behandlingsansvarlige kan overholde sine forpliktelser til å melde bruddet til en kompetent tilsynsmyndighet (Datatilsynet) jf. Personvernforordningen artikkel 33.

3. I overenstemmelse med Vilkår 9, ledd 2, bokstav a skal Databehandleren bistå den Behandlingsansvarlige med å melde bruddet til den kompetente tilsynsmyndigheten (Datatilsynet). Det innebærer at Databehandleren skal bistå med å fremskaffe informasjon listet opp nedenfor, som ifølge personvernforordningen artikkel 33 ledd 3, skal fremgå av den Behandlingsansvarliges melding av bruddet til den kompetente tilsynsmyndighet:

   a. arten av bruddet på personopplysningssikkerheten, herunder, hvis mulig, kategoriene av og omtrentlig antall berørte registrerte samt kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt.
   b. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten
   c. de tiltak som den Behandlingsansvarlige har iverksatt eller foreslår å iverksette for å håndtere brudd på personopplysningssikkerheten, herunder, dersom det er relevant, eventuelt tiltak for å begrense skadevirkninger som følge av bruddet.

4. Partene skal i vedlegg C angi hvilke opplysninger Databehandleren skal fremskaffe i sin bistand til den Behandlingsansvarliges melding av brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

11. Sletting og returnering av personopplysninger

1. Ved avslutning av tjenestene knyttet til behandling av personopplysninger plikter Databehandler å slette alle personopplysninger som er behandlet på vegne av den Behandlingsansvarlige og bekrefte overfor den Behandlingsansvarlige at opplysningene er slettet, med mindre unionsretten eller medlemsstatenes nasjonale lov foreskriver lagring av personopplysningene.
2. Databehandleren forplikter seg til å utelukkende behandle personopplysningene til de(t) formål, med den varighet og under de betingelsene som disse reglene fastsetter.

12. Revisjon, herunder inspeksjon

1. Databehandleren skal stille til disposisjon all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene etter personvernforordningen artikkel 28 og disse Vilkårene. Videre skal Databehandleren muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den Behandlingsansvarlige eller en annen revisor som er bemyndiget av den Behandlingsansvarlige.

2. Prosedyrene for behandlingsansvarliges revisjoner, herunder inspeksjoner, av Databehandler og Underdatabehandlere er spesifisert i vedlegg C.7. og C.8.

3. Databehandleren forplikter seg til å gi tilsynsmyndighetene, som etter gjeldende lovgivning har tilgang til den Behandlingsansvarliges eller Databehandlers lokaler, eller representanter som opptrer på vegne av tilsynsmyndigheten, tilgang til Databehandlerens fysiske lokaler ved presentasjon av behørig legitimasjon.

13. Partenes avtale om andre forhold

1. Partene kan avtale andre bestemmelser som gjelder databehandlertjenesten f.eks. erstatningsansvar, så lenge disse andre bestemmelsene ikke direkte eller indirekte strider mot disse Vilkårene eller til skade for den registrertes grunnleggende rettigheter og friheter og beskyttelse, som følger av personvernforordningen.

14. Ikrafttredelse og opphør

1. Vilkårene trer i kraft på datoen for begge parters underskrift.

2. Begge parter kan kreve Vilkårene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Vilkårene gir grunn til det.

3. Vilkårene gjelder så lenge databehandlertjenesten varer. I denne perioden kan Vilkårene ikke sies opp, med mindre partene avtaler andre Vilkår som regulerer levering av databehandlertjenesten.

4. Dersom levering av databehandlertjenesten opphører og personopplysningene slettes i overensstemmelse med Vilkårene 11.1 og vedlegg C.4, kan Vilkårene sies opp med skriftlig varsel fra begge parter.

5. Underskrift

På veiene av den Dataansvarlige

Dato		Sted	
Navn			
Stilling			
Telefonnummer			
E-post			
Underskrift			

På vegne av Databehandleren

Dato		Sted	Oslo
Navn		Vibeke Jensen Sending	
Stilling		Adm.Dir Hogrefe Norge AS	
Telefonnummer		413 813 05	
E-post		Vibeke.Sending@hogrefe.no	
Underskrift			

15. Kontaktpersoner hos den Behandlingsansvarlige og Databehandleren respektivt

1. *Partene kan kontakte hverandre via kontaktpersonene nedenfor.*
2. *Partene plikter å fortløpende informere hverandre om endringer av kontaktpersoner.*

Navn	
Stilling	
Telefonnummer	
Email	

Navn	Hogrefe Norge AS
Stilling	Support/Vetle Opaas
Telefonnummer	
E-mail	support@hogrefe.no

Vedlegg A Opplysninger om behandling

A.1. **Formålet med Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige**

Å gi den Behandlingsansvarlige mulighet til å vurdere testpersoners psykologiske egenskaper og ferdigheter og/eller følge deres utvikling på individuelt nivå.
Å sammenligne testpersoner med en ekvivalent gruppe i utredning (helse og PPT) eller rekruttering og lederutvikling (HR).

A.2. **Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige angår primært (behandlingens art)**

Administrasjon, skåring og midlertidig lagring av resultater på Hogrefes Testsystem (HTS), inntil data slettes eller overføres i form av PDF eller EXL-fil til journalsystemer eller for videre analyse i forbindelse med forskning.

Databehandlerens levering av testresultater krever løpende oppdatering av at referansestandardene for testapplikasjonene som brukes leverer forventet resultat. Databehandleren eller underdatabehandleren trekker ut anonymisert, tallbasert data fra plattformen (HTS) og analysere disse gruppedata som ledd i kvalitetssikring av testen. Informasjon som trekkes ut er kjønn og alder (hvis relevant) og råskårer (poengsummer per ledd eller område).

I særskilte tilfeller kan den Behandlingsansvarlige unntas fra slik genering av ugjenkallelig anonymisert aggregert data. Valg om å ikke dele slik anonymisert data kan medføre høyere grad av ustabilitet i testene og testresultatene.

Av organisatoriske hensyn ønsker vi å bli unntatt fra å dele anonymisert aggregert data med Hogrefe	☐

A.3. **Behandlingen omfatter følgende typer personopplysninger om de registrerte**

Følgende informasjon kan, men må ikke legges inn på testplattformen:

1. Navn (fornavn og/eller etternavn)
2. E-post adresse for mottak av testlenke (kan også sendes ut på andre måter uten at data lagres i systemet)
3. Fødselsdato

For å unngå å behandle personsensitiv data i HTS må visse innstillinger være satt når plattformen tas i bruk, og alle tester må sendes ut individuelt (ikke bruke gruppeutsendelse).

Følgende informasjon må legges inn:

1. Identifiserende kode
2. Kjønn (visse tester)
3. Alder eller aldersgruppe (visse tester)

Den Behandlingsansvarlige gjøres oppmerksom på at resultatene av psykologiske tester, som behandles i HTS, under visse omstendigheter kan anses som spesielle kategorier av personopplysninger (helseopplysninger). Dette er

spesielt relevant for PPT og Helseforetak, eller private virksomheter som behandler helseopplysninger, men kan også være relevant for den Behandlingsansvarlige i HR- sektoren som bruker tester som ikke er spesifikt utviklet til HR.

A.4. Behandlingen omfatter følgende kategorier av registrerte:

- ☐ den Behandlingsansvarliges ansatte, klienter og ansatte eller jobbsøkere hos klienter
- ☐ forskningsdeltagere
- ☐ studenter
- ☐ elever ved skole eller barn i barnehage når den Behandlingsansvarlige er en skole/barnehage
- ☐ barn, unge og voksne under utredning av PPT
- ☐ barn, unge og voksne under utredning av offentlige institusjoner; NAV, Barneverntjenesten mm. pasienter
- ☐ andre Beskriv:

A.5. Vilkår for start og stopp av behandling av personopplysninger

Databehandlers behandling av personopplysninger på vegne av den Behandlingsansvarlige kan starte etter at Vilkårene trer i kraft ved underskrift. Behandlingen varer inntil avtalen opphører ved skriftlig oppsigelse.

Når den Behandlingsansvarlige manuelt eller automatisk sletter data regnes dette som en instruks til at disse dataene ikke lenger skal behandles. Data vil umiddelbart bli slettet- og kun i visse tilfeller oppbevares i kortere tid enn 14 dager i back-up.

Vedlegg B Underdatabehandlere

B.1. Godkjente underbehandlere

Ved ikrafttredelse av forskriften har behandlingsansvarlig godkjent bruk av følgende underdatabehandlere:

NAVN	ORG. NR.	ADRESSE	BESKRIVELSE AV BEHANDLINGEN
Hogrefe Verlag GmbH & Co. KG,	HRA 3361, Ust.ID: DE160968622	Merkelstrasse 3, 37085 Göttingen, Tyskland,	Hogrefe Verlag GmbH fungerer som utvikler og host for HTS og sikrer at plattformen til enhver tid er operativ. Hogrefe Verlag sikrer sever infrastruktur for å administrere tester, og at tilhørende PDF rapport(er) er tilgjengelig til enhver tid så lenge testdata på en gitt test er tilgjengelig og data ikke er slettet eller kontrakten opphørt. Data oppbevares sikkert og i tråd med denne avtalen og personvernforordningen i Hogrefe Verlags lokaler.

Hogrefe Verlags databehandlingsvirksomhet er overvåket av ekstern DPO, Felix Hudy, Administrerende konsulent Datenschutz (Databeskyttelse), som kan kontaktes via privacy@hogrefe.com

Ved ikrafttredelse av Vilkårene har den Behandlingsansvarlige godkjent bruk av ovennevnte underbehandlere for den beskrevne behandlingsaktiviteten. Databehandleren kan ikke – uten den Behandlingsansvarliges skriftlige godkjenning – benytte en underdatabehandler til annen behandlingsaktivitet enn den som er beskrevet og avtalt eller benytte en annen underdatabehandler til denne behandlingsaktiviteten.

B.2. Melding om godkjenning av underbehandlere

Databehandler informerer den Behandlingsansvarlige om eventuelle endringer i bruken av underdatabehandlere med minimum 30 dagers varsel, og gir derved den Behandlingsansvarlige mulighet til å protestere mot endringen. Ved manglende aksept av endringer i bruk av underdatabehandlere, kan avtalen sies opp.

Vedlegg C Instrukser vedrørende behandling av personopplysninger

C.1. **Gjenstand for behandlingen/instruksjonene**

Databehandleren og søstervirksomheter av Databehandleren (andre Hogrefe Forlag) utvikler vitenskapelig baserte psykometriske tester for å kartlegge psykologiske egenskaper og ferdigheter primært innenfor det pedagogisk-psykologiske området, det psykologisk-kliniske området, samt Ledelse - og rekrutteringsområdet (HR), og stiller disse testene til rådighet for den Behandlingsansvarlige i internettapplikasjonen Hogrefe Test System (HTS).

HTS portalen er utviklet til å samle inn respons på normerte psykometriske testere, skåre responsene i testportalen på en vitenskapelig og pålitelig måte og danner rapporter i PDF-format for videre tolkning av resultater av sertifiserte testledere.

Tilgang til portalen og testene er avhengig av den Behandlingsansvarliges sertifiseringer og brukertillatelse, og den Behandlingsansvarlige er selv ansvarlig for at alle som får tilgang til portalen har tilstrekkelig kompetanse til å administrere gjeldende tester.

Alle brukerkontoer er personlige og skal kun brukes av personen hvis navn er tilknyttet kontoen. Brukeren og i ytterste tilfelle den Behandlingsansvarlige (administrator/virksomheten) er ansvarlig for ikke å dele passord med andre, eller gi tilgang til plattformen. Bruker må legge inn personlig passord og aktivere to-faktor autentifisering, ved første pålogging for å sikre data.

Den Behandlingsansvarliges ansatte (individuelle brukere) har ansvar for å velge ut hvem som skal delta i testen samt testene den enkelte skal delta i. Hvilken test og hvordan testen skal gjennomføres. Alle testkompetente personer er personlig ansvarlig for å følge de internasjonale testetiske retningslinjene (ITC-ethical guidelines) i kjøp, valg, administrasjon og tolkning av verktøyene som leveres i HTS. Dette gjelder også beskyttelse av testens innhold under åndsverkloven.

Den Behandlingsansvarlige er ansvarlig for å følge personvernforordningen, landets lover og disse Vilkårene når det kommer til hva, hvilken og hvordan informasjon legges inn i HTS-portalen. I tillegg er den Behandlingsansvarlige ansvarlig for hvordan data behandles etter den forlater HTS-portalen i form av et PDF-dokument eller migrert data i form av XML-fil til forskning (Article 4 (7) GDPR).

Hver testperson (de som får sin personinformasjon behandlet) får et unikt passord for å få tilgang til portalen www.Hogrefe-online.com. I visse tilfeller (HR-versjonen) kan en felles lenke sendes ut til alle testpersoner. Når testpersonen åpner lenken skapes det en unik kode (TAN kode) i neste ledd, som gir han/hun eksklusiv adgang til egen test.

Den Behandlingsansvarlige og dens ansatte er ansvarlig for at testpersonen - og i den grad det er nødvendig - foresatte eller verge - har mottatt tilstrekkelig opplysninger i forkant av testen. Som minimum skal disse opplysningene inneholde formål med databehandlingen, hvordan data oppbevares, hvem som har tilgang og når data slette. Nødvendig aktivt (vedkommende foretar seg en handling) informert samtykke skal innhentes. Det er mulig å opprette et eget standard samtykkeskjema i portalen.

HTS-systemet beregner resultater basert på testpersonenes unike svar, lagrer data for den Behandlingsansvarlige og, med mindre annet er avtalt, trekker ut statistiske oppsummeringer som referansegrunnlag for normene.

Den Behandlingsansvarlige gjøres oppmerksom på at resultatet av psykologiske tester under visse omstendigheter kan kategoriseres som automatisk behandling/avgjørelse og profilering som personer er beskyttet mot under personvernforordningen artikkel 29 (jfr. EU-forordning 2016/679 av 27. april 2016). Profilering skal her forstås som automatisk analyse eller prediksjon ved enkeltpersoner eller grupper inkl. analyse av arbeidsprestasjon eller forventet arbeidsprestasjon, helse og atferd. Dette gjelder spesielt for tester som gir klare entydige svar som konklusjon eller som er diagnostiske. Risiko for uetisk og feil behandling er stor ved automatisk utsendelse av data, eller ved å gi fra seg rådata til personer uten tilstrekkelig kompetanse.

Den Behandlingsansvarlige må sikre at resultatet fra HTS ikke sendes ut uten tilstrekkelig menneskelig behandling av data i form av tolkning som oppsummeres i en tolkningsrapport eller muntlig eller skriftlig tilbakemelding/tilbake lesing i HR, og at kun rapporter som kan deles med mottaker (tilpasset mottaker) deles, samt at det gis tilstrekkelig informasjon i hvilken grad informasjonen er vektet i endelig konklusjon eller prediksjon.

I tillegg må den Behandlingsanvarlige være observant på rettighetshavers rett til beskyttelse av åndsverk og konsekvenser ved brudd på åndsverkloven gjennom å dele innhold i tester med uvedkommende eller kopiere/inkludere det i egne digitale plattformer uten tilstrekkelig tillatelse.

C.2. Behandlingssikkerhet

Behandlingen kan omfatte en stor mengde personopplysninger, som enten i sin isolerte eller aggregerte form må anses som konfidensiell, som det er iverksatt et tilstrekkelig sikkerhetsnivå for.

Databehandler har rett og plikt til å ta beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som må iverksettes for å etablere nødvendig (og avtalt) sikkerhetsnivå.

For oversikt over organisasjonens tekniske og organisatoriske tiltak se vedlegg D. Store og betydningsfulle endringer blir dokumentert og den Behandlingsansvarlige vil motta skriftlig varsel. Databehandleren må imidlertid – under alle omstendigheter og som et minimum – iverksette følgende tiltak, som er avtalt med den Behandlingsansvarlige:

FYSISK TILGANGSIKRING

- Underdatabehandleren har bedriftsinterne forskrifter om sikkerhetstiltak. Det bedriftsinterne regelverket og retningslinjene gjennomgås minst en gang i året.
- Server(e) er fysisk plassert i en lås- og adgangskortsikret rom med klimaanlegg og sikret strømforsyning. Serverrom er videoovervåket og beskyttet av brann- og tyverialarm. Brannslukningsapparater er plassert i nærheten av serverrommet.
- Alle arbeidsplasser er sikret mot uautorisert tilgang til personopplysninger, blant annet med inngangssikkerhet, adgangskort, alarmer og begrenset adgang til serverrom i tråd med personvernforordningen Artikkel 28 (3) (b).

SIKRING AV DATA PÅ INTERNET OG UNDER OVERFØRING

Databehandleren legger vekt på konfidensialitet av personsensitiv data og å følge GDPR. Følgende tiltak er iverksatt av underdatabehandleren for å sikre data mot tap, skade, uautorisert adgang eller feil bruk.

- Alle eksterne kommunikasjonsforbindelser er sikret mot uautorisert tilgang til personopplysninger. Kommunikasjon med server(e) (Hogrefe-online.com) foregår utelukkende via krypterte SSL-forbindelser.
- Server(e) har sikkerhetssertifikat.
- Det brukes en form-basert autentifiseringsprosess
- Data overføres via TLS-kryptert forbindelse (TLS-encrypted connection).
- Den Behandlingsansvarliges tilgang beskyttes av alfanumerisk passord (åtte tegn).
- To faktor-autentifisering kan aktiveres ved første pålogging (men er ikke automatisk aktivert)
- Administrasjonsplattformen (nettbasert portal) har sitt eget brukerstyringssystem som sikrer at kun data som skal være synlig for brukeren er synlig for brukeren.
- Datasenteret har «redundant data Connectivity» som betyr at data kan fortsette å strømme inn og ut selv om det er en feil i deler av systemet.
-

SIKRING AV DATA UNDER OPPBEVARING

- Databehandlerens og underbehandleres ansatte som behandler personopplysningene har mottatt nødvendig informasjon om behandlingen av personopplysningene i tråd med personvernforordningen artikkel 28 (3) (b).
- Databehandleren og underbehandleres ansatte kan kun få tilgang til og gjøre seg kjent med personopplysninger i den grad det er nødvendig for å levere service knyttet til drift og bruk av HTS. Ansatte tildeles differensiert tilgang og har dermed kun tilgang til arbeidsrelevante systemer.
- Databehandleren og underbehandleres ansatte er underlagt taushetsplikt om de behandlede dataene.
- Tilgang til servere/data er begrenset til relevante ansatte ved Databehandleren og underdatabehandlere med unik og personlig pålogging. Det er etablert prosedyrer for å gi og trekke tilbake adgangstillatelser.
    i. Tilgang til server(e) er begrenset til port 443
    ii. Server(e) er beskyttet av brannmur. Systemer er av typen Linux og databasesystemet er av typen MariaDB.
    iii. Alle kundedatabaser er fullstendig kryptert.
    iv. Databasen er kontinuerlig kopiert (backed up) på separat maskinvare.
    v. Databærende utstyr, i utgangspunktet kun harddisker, kastes når det returneres til distributøren eller destrueres av et eksternt selskap i henhold til sertifisert standardprosedyre for å sikre at personopplysninger ikke er tilgjengelige.

EVNE TIL Å GJENOPPRETTE TILGJENGELIGHETEN OG TILGANG TIL PERSONOLPPLYSNINGER VED FYSISK ELLER TEKNISK HENDELSE

- Tilgang til og inntasting og sletting av data logges. Bruk av systemet logges og analyseres. Loggen lagres på ubestemt tid, men anonymiseres etter 4 uker.
- Personopplysningene er sikkerhetskopiert. Sikkerhetskopien lagres kryptert, separat og under samme sikkerhetstiltak som originaldataene. Sikkerhetskopier oppbevares i 14 dager.
- Adkomst og andre sikkerhetstiltak overvåkes kontinuerlig i henhold til foreskrevet prosedyre. De enkelte komponentene i systemene testes rutinemessig.

På instruks fra den Behandlingsansvarlige kan Databehandler sende eller motta data i ukryptert form i forbindelse med support og annen service.

C.3 **Bistand til den Behandlingsansvarlige**

Databehandler skal så langt det er mulig – innenfor omfanget beskrevet nedenfor – bistå den Behandlingsansvarlige i henhold til Vilkårene 9.1 og 9.2 ved å iverksette følgende tekniske og organisatoriske tiltak:

- Dersom Databehandleren og underdatabehandleren mottar tilgangsforespørsler eller andre rettighetsforespørsler i henhold til personvernforordningen, henvises de til den Behandlingsansvarlige. Databehandleren bistår på den Behandlingsansvarlige instruks med oppfyllelse av rettighetsforespørsler.
- Som en del av sin personvernpolicy har underdatabehandleren på vegne av databehandleren en beredskapsplan for sikkerhetshendelser og begge parter bistår som en del av dette kunden med å rapportere potensielle sikkerhetsbrudd til relevante myndigheter, som utgangspunkt Datatilsynet, samt utbedre disse.

C.4 Oppbevaringsperiode/sletterutiner

Personopplysninger lagres etter instruks fra den Behandlingsansvarlige og i tillegg i henhold til avtalens varighet.

Når Avtalen om behandling av personopplysninger opphører skal Databehandler slette personopplysningene i henhold til Vilkårene 11.1, med mindre den Behandlingsansvarlige – etter signering av disse Vilkårene – har endret opprinnelige valg. Slike endringer skal dokumenteres og lagres skriftlig, herunder elektronisk, i tilknytning til regelverket.

Hvis ikke annet avtales under slettes data 30 dager etter kontrakten opphører. Den Behandlingsansvarlige og dens ansatte har også tilgang til fortløpende å slette egne data og er ansvarlig for å overholde eventuelle slettefrister.

Alternativ instruks om sletting av data ved oppsigelse/opphør	‘

C.5 Behandlingssted

Behandling av personopplysningene omfattet av Vilkårene kan ikke skje uten skriftlig forhåndsgodkjenning fra den Behandlingsansvarlige på andre steder enn følgende:

- Server(e) er fysisk plassert på og andrelinjesupport utføres på følgende adresse: Hogrefe Verlag GmbH & Co. KG, Merkelstrasse 3, 37085 Göttingen, Tyskland.
- 1. trinns support gjennomføres på følgende adresse: Hogrefe Norge AS, Oscars Gate 35 A, 0258 Oslo, Norge

C.6 Instruksjoner vedrørende overføring av personopplysninger til tredjeland

Dersom den Behandlingsansvarlige i disse Vilkårene eller i ettertid ikke gir en dokumentert instruks om overføring av personopplysninger til et tredjeland, har ikke Databehandleren rett til å gjennomføre slike overføringer innenfor rammen av disse Vilkårene.

C.7 Prosedyrer for den bBehandlingsansvarliges revisjoner, herunder inspeksjoner, med behandling av personopplysninger overlatt til Databehandler

Databehandler skal årlig for egen regning utarbeide en erklæring om Databehandlerens etterlevelse av personvernforordningen, gjeldende personopplysningsbestemmelser i unionsretten eller i medlemsstatenes nasjonale rett og disse vilkårene.

Den Behandlingsansvarlige eller en representant for den Behandlingsansvarlige har også adgang til å foreta inspeksjoner, herunder fysiske kontroller, på de stedene Databehandleren behandler personopplysninger, herunder fysiske steder og systemer som brukes til eller i forbindelse med behandlingen. Slike kontroller kan foretas når den Behandlingsansvarlige finner det nødvendig.

Den Behandlingsansvarliges eventuelle utgifter i forbindelse med fysisk kontroll bæres av den Behandlingsansvarlig selv. Databehandleren er imidlertid forpliktet til å bevilge de ressursene (hovedsakelig i form av tid) som er nødvendig for at den Behandlingsansvarlig kan gjennomføre sin kontroll.

C.8 Prosedyrer for revisjoner, inkludert inspeksjoner, med behandling av personopplysninger overlatt til underbehandlere

Databehandleren skal årlig for egen regning utarbeide en erklæring om underdatabehandlerens etterlevelse av personvernforordningen, nasjonale lover og disse Vilkårene. Dette kan gjøres sammen med rapporten beskrevet i punkt C7.Basert på resultatene av erklæringen har den Behandlingsansvarlige rett til å be om iverksetting av ytterligere tiltak for å sikre samsvar med personvernforordningen, nasjonale lover og disse Vilkårene.

Databehandleren eller en representant for Databehandleren har også adgang til å foreta inspeksjoner, herunder fysiske inspeksjoner, på de stedene som underdatabehandleren behandler personopplysninger fra, herunder fysiske steder og systemer som brukes til eller i forbindelse med behandlingen. Slike kontroller kan foretas når Databehandleren finner det nødvendig. Dokumentasjon for slike kontroller oversendes uten ugrunnet opphold til den Behandlingsansvarlig til orientering.

Den Behandlingsansvarlig kan – dersom det anses nødvendig – velge å iverksette og delta i en fysisk kontroll av underdatabehandleren. Dette kan bli aktuelt dersom den Behandlingsansvarlige vurderer at Databehandlers inspeksjon av underdatabehandler ikke har gitt den Behandlingsansvarlige tilstrekkelig sikkerhet for at behandlingen hos underdatabehandler er i samsvar med personvernforordningen eller medlemsstatenes nasjonale lover og disse Vilkårene.Den Behandlingsansvarliges eventuelle utgifter i forbindelse med fysisk kontroll av underdatabehandler bæres av den Behandlingsansvarlig selv. Databehandleren og underdatabehandleren er imidlertid forpliktet til å bevilge de ressursene (hovedsakelig i form av tid) som er nødvendig for at den Behandlingsansvarlig kan gjennomføre sin kontroll.

Den Behandlingsansvarliges eventuelle deltakelse i en inspeksjon hos underdatabehandler endrer ikke det faktum at Databehandler også deretter har det fulle ansvar for at underdatabehandleren overholder personvernforordningen eller medlemsstatenes nasjonale lover og disse Vilkårene.

Vedlegg D Technical and organizational measures from Hogrefe Verlag GmbH

1. Confidentiality (Article 32 (1) (b) GDPR)

(1) Physical Access Control

Scope
The objective of physical access control is to prevent unauthorized persons from getting close to data processing equipment, thereby gaining physical access to the systems used to process or use personal data by implementing various structural, organizational and personnel measures, which shall be laid down in a physical access control policy.

Technical and organizational measures
The purpose of the following measures is to deny an unauthorized individual physical access to data processing equipment:

- Security passes
- Electronic access code cards / access transponders
- Rules for granting access authorisation
- Video surveillance
- Alarm system
- Keys policy
- Visitors must always be accompanied by employees
- Visitor check-in/check-out records
- Tiered security areas and controlled access
- Separately secured access to the data centre
- Servers are kept in locked rooms
- Data carriers are kept under lock and key or in locked rooms
- Data backups (e.g. tapes, CDs) are kept in an access-protected safe

(2) Equipment access control

Scope
The objective of equipment access control is to deny an unauthorized individual access to data processing equipment by implementing appropriate measures to ensure that only users who have the appropriate authorization can gain access to data and IT applications. If a user fails to demonstrate that he or she has the necessary authorization, the equipment access control will deny the user access to the IT system.

Technical and organizational measures
The purpose of the following measures is to deny an unauthorized individual access to data processing systems:

- Password protection of workstation screens
- Functional and/or temporary allocation of user authorisations
- Use of individual passwords
- Automatic blocking of user accounts after entering the wrong passport multiple times
- Automatic password-protected screen lock after a period of inactivity (screensaver)
- Password policy and minimum password complexity requirements:
  - at least 8 characters / upper and lower case, special characters, number (min. 3 criteria)
  - Users deterred from using easy-to-guess passwords (e.g. Dog1, Dog2, Dog3)
  - Password history (users are prohibited from repeating 5 last passwords)

- Procedure for granting authorizations to new employees
- Procedure for withdrawing authorizations from employees who move to a different department
- Procedure for withdrawing authorizations from employees who leave the company
- Confidentiality obligation
- Logging and evaluation of system use
- Controlled destruction of data carriers

(3) Data access control

Scope

The objective of data access control is to ensure that those authorized to use a data processing system can only access data covered by their access authorization, and personal data is not read, copied, modified, or removed by an unauthorized user during processing, use or after it has been stored.

Technical and organizational measures

The purpose of the following measures is to deny an unauthorized individual access to data processing systems:

- Formulation of access authorization policy
- Procedure for the recovery of data from backups (who, when, at whose request)
- Regular review of authorizations
- Restriction of free and uncontrolled query options for databases
- Regular analysis of logs (log files)
- Partial access to databases and functions (read, write, execute)
- Logging of file access
- Logging of file erasures
- The company uses adequate security systems (software/hardware), including:
  - Virus scanner
  - Firewalls
  - SPAM filter
  - Intrusion prevention (IPS)
  - Intrusion detection (IDS)
- Encrypted storage of data
- Use of hash function – SHA2 (256, 384, 512 bit)

(4) Separability

Scope

The objective of the principle of separability is to ensure that data collected for different purposes can be processed separately. Among other things, the purpose is to have the ability to associate data with a specific department, individual, branch or customer, and to comply with the principle of purpose limitation, which is one of the basic principles of data protection. The objective can be achieved in many ways, for example, by implementing a suitable application authorization policy.

Technical and organizational measures

The purpose of the following measures is to ensure that data collected for different purposes is processed separately:

- Separation of customers (multi-controller capability of the system used)
- Logical data separation (e.g. based on customer or Controller numbers)
- The Controller's and other customers' data are processed by different employees of the Processor
- Access authorisation policy which takes into account the requirement of processing Controller's data separately from other customers' data
- Segregation of functions

- Separation of development, testing and production systems
- Dedicated system
-

(5) Pseudonymization

The Controller can configure the system settings to ensure that the processing of personal data takes place in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

2. Integrity (Article 32 (1) (b) GDPR)

(1) Data transfer control

Scope
The objective of data transfer control is to ensure that personal data cannot be read, copied, modified or removed without authorisation during their transfer or transport or when storing the data on data carriers, and that it can be checked and determined who are the recipients of the personal data transfer.

Technical and organizational measures
The following measures have been implemented to achieve this objective:

- The use of https connections for data exchange
- Safe destruction of paper documents by using sealed metal containers (data protection bins) and documented disposal by service providers

(2) Input control

Scope
The objective of input control is to ensure that it is possible to check and establish whether and by whom personal data has been input into data processing systems, modified or removed.

Technical and organizational measures
The following measures have been implemented to achieve this objective:

- Identification of acquired data
- Definition of user authorizations (profiles)
- Differentiated user access authorizations:
  - Read, change, delete
  - Partial access to data or functions
  - Field access to databases
- Organisational specification of input responsibilities
- Logging of entries/erasures
- Obligation to maintain data confidentiality
- Log policy that goes beyond the OS standard

3. Availability and resilience (Article 32 (1) (b) GDPR)

(1) Availability control

Scope
The objective of availability control is to ensure that personal data are protected against accidental destruction or loss.

Technical and organizational measures
The following measures have been implemented to achieve this objective:

- Data backup policy
- Implementation of the data backup strategy
- Access to server rooms restricted to necessary personnel
- Fire alarm systems in server rooms
- Smoke detectors in server rooms
- Waterless firefighting systems in server rooms
- Air-conditioned server rooms
- Lightning/surge protection
- Water sensors in server rooms
- Server rooms located in separate fire-containment sections
- Backup systems located in separate rooms and fire-containment sections
- Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.)
- CO2 fire extinguisher in the immediate vicinity of the server rooms
- Storage of data in data cabinets, safes
- UPS system (uninterruptible power supply)

(2) Resilience and reliability control

Scope
The objective of resilience and reliability control is to ensure that systems can handle risk-related changes and have the ability to tolerate and withstand disruptions.

Technical and organizational measures
The following measures have been implemented to achieve this objective:

- Redundant power supply
- Redundant UPS system
- Redundant air conditioning
- Hard disk mirroring
- Data storage on RAID systems (RAID 1 and higher)
- Demarcation of critical components
- Performance of penetration tests
- System hardening (deactivation of unnecessary components)
- Immediate and regular activation of available software and firmware updates
    - Identification of the different devices that make up the network and identification of their hardware version as well as their current software and firmware versions.
    - Communication with manufacturers to learn about new updates and patches released for the company's devices.
    - Setting aside periods for installing updates (e.g. less busy periods, maintenance, etc.).
    - Use of redundant systems to maintain operations while the main devices are being updated.
    - Progressive deployment of updates/patches to detect problems early without compromising multiple devices.

  - Setting aside a testing period to verify the correct implementation of the update and ensure that operations continue to run smoothly following the update.
- Security is among the key aspects taken into account when designing systems:
  - Limitation of authorizations on a need-to-know basis.
  - External processors and maintenance personnel receive a specific access authorization that is only activated during the intervention and deactivated for the rest of the time.
- Regular awareness-raising campaigns to inform users about security policies, both for specific systems and legacy IT systems.

4. Process for regularly testing, assessing, evaluating (Article 32 (1) (d) GDPR; Article 25 (1) GDPR)

(1) Control processes

We have implemented the following processes for regularly testing, assessing and evaluating the effectiveness of data security measures:

- Reporting of new/changed data processing procedures to the DPO
- Recording of processes for reporting new/changed procedures
- Selection of data protection-friendly default settings
- Subjecting the implemented protection measures to regular internal controls

(2) Processing control

Scope

The objective of processing control is to ensure that personal data processed by service providers on behalf of the Controller (subprocessors) can only be processed in compliance with the Processor's instructions.

Technical and organizational measures

The following measures have been implemented to achieve this objective:

- Contracts drafted in accordance with legal requirements (Article 28 GDPR)
- Central recording of existing service providers (standard contract management)
- Regular checks by the Processor after the contract start date (during the term of the contract)
- Inspections at the premises of the Processor
- Verification of the Processor's data security concept
- Review of the Processor’s existing IT security certificates