Konsekvensbedömning enligt Dataskyddsförordningen (DPIA)

Netpublicator Sign - Elektronisk underskrift för nämnd- och utskottshandlingar

2023-05-09

Konsekvensbedömning	Förhandssamråd	Inlagda i Myndighetens förteckning
☐Underlag ☒Genomförd ☐Granskad av DSO[1]	☐ Underlag ☐ Granskad av DSO ☐ Godkänd av informationsägaren ☐ Genomfört	☐ Underlag ☐ Förtecknad ☐ Granskad av DSO ☐ Godkänt av informationsägaren

Versionshantering

Datum	Version	Beskrivning	Ändrat av
20230307	0.1	Utkast	Tove Artonius
20230509	1.0	Genomförd	Marcus Andersson

Medverkande

Namn	Roll
Marcus Andersson	Utvecklingsledare, ärendehantering
Camilla Porshede Johansson	Utvecklingsledare, dataskydd

Innehåll

1 Grundläggande uppgifter

Om en tröskelanalys för konsekvensbedömning har genomförts, vänligen beskriv samma svar under detta avsnitt ett som i tröskelanalysen från 1.1 till 1.15. Även kan mycket grundläggande uppgifter hämtas från PU-registret om behandlingen redan finns beskriven där.

1.1 Tidigare konsekvensbedömning (DPIA)

Detta är en:

☒ ny konsekvensbedömning

☐ komplement till en tidigare konsekvensbedömning (DPIA)

Har någon annan gjort en liknande konsekvensbedömning för tekniken som används eller liknande aktiviteter?

Är behandlingens art, omfattning, sammanhang och ändamål mycket lika en behandling för vilken en konsekvensbedömning har utförts?

☒ Ja

☐ Nej

☐ Inte säker

Beskriv och kommentera ditt svar nedan:

Äldre samt vård- och omsorgsförvaltningen har genomfört konsekvensbedömning med rubriken Netpublicator Sign - Elektronisk underskrift för nämnd- och utskottshandlingar.

1.2 Uppgifter om kontaktperson för bedömningen

Namn:

Marcus Andersson

Organisation/Enhet:

Förvaltningen för funktionsstöd

E-post:

marcus.andersson@funktionsstod.goteborg.se

Telefonnummer:

031-365 32 44

1.3 Namn på bedömningen

Netpublicator Sign – Elektronisk underskrift för nämnd- och utskottshandlingar.

Behandlingens namn hjälper till att skilja registreringen från andra och behöver vara unik, men inte för lång.

Normalt är namnen på behandlingen redan satt i PU-registret och samma namn ska användas här.

Exempel "Hantera tillträde till lokalerna", "Kompetensutveckling – Intraservice", ”Hantera personaladministration – Visuell kommunikation", ”Semesterschema" eller "Medlemsregister".

Digital signering av nämnd- och utskottshandlingar sker inom de båda behandlingarna:

- Beslut som fattas av nämnd/utskott med stöd av kommunallag och/eller socialtjänstlag.

- Myndighetsutövning mot enskild. (myndighetsutövning mot enskilda kan ske)

Behandlingarna struktureras i förvaltningen för funktionsstöds personuppgiftsregister under processen 1.1 Utföra politiskt ledningsarbete. Personuppgiftsregistret förs i verksamhetssystemet DraftIT.

I process 1.1 ligger det politiska arbetet, processen avser bland annat beslutsfattande/rapportering hos nämnd/styrelse. Processen omfattar även övergripande styrdokument och uppdrag för nämnder och bolag.

Denna konsekvensbedömning är gemensam för båda behandlingarna då det inom de båda behandlingarna hanteras känsliga personuppgifter och bedömningen i huvudsak är identisk. Om beskrivningarna i kommande avsnitt skiljer sig åt tydliggörs det i det avsnittet.

1.4 Ändamål med behandlingen

Beskriv tydligt varför behandlingen utförs – ändamålet. Med detta menas det huvudsakliga syftet med hanteringen av uppgifterna.

Ändamålet styr vilka personuppgifter som får ingå, vilka personer som får ha tillgång till informationen och när personuppgifterna ska gallras. En behandling av personuppgifter kan ha flera ändamål. Eventuella ytterligare ändamål beskriver du under *3.1.13.1.1Ytterligare ändamål* nedan.

Exempel: "Lönekörningar och administration av löneutbetalningar och källskatteavdrag. Inbetalning av skatter och sociala avgifter".

Övergripande ändamål med behandlingen är följsamhet mot kommunallag genom att nämndprotokoll ska justeras senast fjorton dagar efter sammanträde 6 kap. 6 § 35. Att signera nämndprotokoll digitalt och därmed även på distans har som syfte att effektivisera handläggningsprocessen genom minskad arbetsbörda, minskad miljöpåverkan samt kortare ledtider från protokollföring till justering.

Införandet av elektroniska underskrifter görs även för att vid pandemi möjliggöra minimering av smittorisk för grupper som annars skulle behöva resa och vistas i kontorslokaler för att underteckna dokument.

1.5 Bakgrund (processbeskrivning)

Här ska en systematisk beskrivning av hur personuppgifterna kommer hanteras framgå. I detta avsnitt kan det vara bra att lägga in en beskrivning av processen som personuppgifterna behandlas i. Ett annat tips är att lägga med en flödesanalys av hur personuppgifterna kommer flöda i systemet. Syftet är med andra ord att läsaren efter detta avsnitt ska förstå hur ni kommer behandla alla personuppgifterna i processen/systemet.

Här räcker det med en kort summering. Konkreta detaljer kommer samlas in i frågorna nedan.

Till exempel:

Vad gör du och varför?

I vilket sammanhang görs bedömningen?

Vem är ansvarig eller ägare?

Vilka informationsbärare (system eller annat) används?

Handling upprättas på tjänstepersonens dator enligt ordinarie rutin, till exempel att tjänsteperson skapar ett protokoll enligt mall. Tjänsteperson loggar in i Netpublicator Sign och laddar upp handlingen till signeringsdelen och skickar signeringsbegäran till behörig signerare. Signeraren tar emot begäran, loggar in med mobilt BankID, granskar handlingen och väljer att avfärda och invänta ny handling, eller att skriva under. Signeraren skriver under handlingen med mobilt BankID. Tjänsteperson loggar in i Netpublicator och hämtar undertecknad handling. Diarieför den undertecknade handlingen. Tjänsteperson tar därefter bort handlingen från Netpublicator Sign. I Netpublicator Sign har endast de personer som lagts in som behöriga för att signera just det dokumentet behörighet. Avgränsning: Handlingar som hanteras i mötesdelen (den del där politiker tar del av handlingar inför sammanträden) och omfattas inte av denna konsekvensbedömning.

1.6 Personuppgiftsansvarig – PUA (organisation)

Skriv in vilken eller vilka organisationer (gemensam personuppgiftsansvarig) som är ansvarig för den aktuella personuppgiftsbehandlingen.

Förvaltningen för funktionsstöd

1.7 Kontaktperson (hos PUA/infoägare/processägare)

Skriv in den som ska vara kontaktperson (informationsägaren) på myndigheten för aktuell behandling.

Avdelningschef Maria Berntsson

1.8 Ansvarig chef

Detta kan vara verksamhetschef, enhetschef, avdelningschef, kanslichef eller förvaltningschef.

Avdelningschef Maria Berntsson

1.9 Verksamhetsområde

Ange vid vilka avdelningar eller verksamhetsområden som behandlingen finns och, om möjligt, vilken enhet eller grupp.

Stab, kommunikation och säkerhet

1.10 Rättslig grund (art 6)

Vilken av följande rättsliga grunder används för behandlingen?

☒ Myndighetsutövning och uppgift av allmänt intresse
☐ Rättslig förpliktelse
☐ Avtal med den registrerade
☐ Skydda grundläggande intresse
☐ Intresseavvägning
☐ Samtycke

Beskriv och kommentera ditt svar nedan:

Nämnden och utskottet fattar beslut enligt gällande lagstiftning och nämndens delegationsordning. Nämndprotokoll lyder under den lagliga grunden uppgift av allmänt intresse. Utskottsprotokoll innefattar myndighetsutövning mot enskild och kan i vissa fall vara av allmänt intresse. Digital signering av nämndhandlingar har efterfrågats av de förtroendevalda politikerna för att förenkla signeringsförfarandet.

Digitalisering av nämnd- och utskottsprotokoll ligger i linje med regeringens digitaliseringspolitik som innebär att Sveriges offentliga förvaltningar ska arbeta för digitalisering i effektiviserings- och tillgänglighetssyfte. Denna del av personuppgiftsbehandlingen lyder under den lagliga grunden allmänt intresse.

1.11 Kategorier av personuppgifter

Vilka kategorier av personuppgifter behandlas?

Se ***Appendix 2 – Lista på personuppgiftskategorier*** för detaljerad information om vad de olika kategorierna exempelvis innehåller.

☒ Anställningsinformation
☐ Arbetsmiljö
☐ Bakgrundskontroller
☐ Biometriska och genetiska uppgifter
☒ Inloggningsuppgifter
☒ Familjeinformation
☒ Finansiella uppgifter
☐ Kontaktinformation
☒ Myndighetsutfärdad identifikation
☒ Personlig identifikation
☐ Resor och kostnader
☐ Sociala medier
☐ Sociala välfärdsdata
☒ Personliga egenskaper, utbildning och arbete
☒ Tekniska metadata
☐ Annat

Beskriv och kommentera ditt svar nedan:

Tekniska metadata utifrån signering.

Anställningsinformation kan innehålla namn och befattning av de tjänstepersoner som är med på mötena.

Information om partitillhörighet för deltagande politiker förekommer i protokollen.

Med myndighetsutfärdad identifikation avses personnummer.

Underskrift i Netpublicator Sign innehåller uppgift om bank.

Familjeförhållande och andra personliga bakgrundsfakta förekommer i utskotts-protokollen.

Personliga egenskaper kan förekomma i form av uppgifter om utbildning, bete-ende, umgängesliv och personliga kontakter.

I de individärenden som kan förekomma i utskottsprotokoll förekommer namn, personnummer och namn på adress i form av beslut om boende enligt SoL och LSS och berör behandlingen myndighetsutövning mot enskild.

1.12 Kategorier av registrerade

Vilka kategorier av registrerade finns i registret/behandlingen?

- ☒ Anställda
- ☐ Kunder
- ☒ Leverantörer
- ☒ Besökare
- ☐ Elever
- ☐ Patienter
- ☒ Medlemmar
- ☒ Invånare
- ☐ Konsulter
- ☐ Asylsökande
- ☒ Personer med funktionsvariation
- ☒ Annat

Beskriv och kommentera ditt svar nedan:

Med annat avses förtroendevalda och ombud.

Namn på medlemmar i exempelvis brukarföreningar kan förekomma i nämnd-protokollen.

Namn på leverantörer kan förekomma i nämndprotokollen.

Uppgifter om personer med funktionsvariation förekommer i utskottsprotokollen och berör behandlingen myndighetsutövning mot enskild.

1.13 Antal registrerade

Hur många registrerade inkluderas i behandlingen?

- ☐ 1-100
- ☒ 101-1000
- ☐ 1001-5000
- ☐ 5001-10000
- ☐ 10001-50000
- ☐ 50001 <
- ☐ Annat

Beskriv och kommentera ditt svar nedan:

Detta är en uppskattad siffra per år.

1.14 Publikt tillgängliga uppgifter

Är någon data redan publikt tillgänglig?

OBS: Om personuppgifterna redan är insamlade, var de publikt tillgängliga vid tiden för insamlingen?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Förtroendevaldas partitillhörighet.

1.15 Tillgång till personuppgifter

Vilka tjänstemän och andra roller kommer ha tillgång till uppgifterna?

☐ En person
☒ Ett fåtal handläggare
☒ Personal inom enheten
☒ Personal inom förvaltningen
☐ Personal inom staden
☒ IT-administratörer
☒ Leverantörer
☒ Annat

Beskriv och kommentera ditt svar nedan:

Med annat avses förtroendevalda. Ordförande, justerare och i förekommande fall sekreterare som signerar protokollet. Med personal inom enheten samt ett fåtal handläggare avses två nämndsekreterare, utvecklingsledare och registratorer inom förvaltningen. Med personal inom förvaltningen avses personal inom förvaltningsledningen. Med IT- administratörer avses systemförvaltare inom Intraservice. Med leverantör menas Netpublicator som tillhandahåller tjänsten Netpublicator Sign.

1.15.1 Tillgång till personuppgifter (omfattning)

Ange hur många anställda som kommer ha tillgång till hela och de olika delarna av behandlingen om det är relevant.

Politiker 3 st.

Inom förvaltningen 5 st tjänstepersoner.

Intraservice har cirka 2 st med behörighet och tillgång till systemet. Loggar kan begäras ut av Netpublicator.

Netpublicator personal 1 konto.

1.16 Informationsbärare

Ange vilka informationsbärare (system) som används för behandlingen.

Applikationen Netpublicator Sign, tjänstepersons dator eller mobila enhet. Förtroendevaldas dator eller mobila enhet, kan vara privata enheter. Stadens tillhandahållna enheter rekommenderas, men det finns inga hinder för privata enheter.

1.17 Lagring (Dokumenthanteringsplan)

Ange punktnotation och rubrik enligt förvaltningens klassificeringsstruktur nedan. Gallringsbeslut i dokumenthanteringsplanen anger tidsgränser för data som ska bevaras, rensas eller gallras.

Nämndprotokoll och utskottsprotokoll ingår under punktnotation 1.1 i klassificeringsstruktur för nämnden för funktionsstöd version 1:1:2021.

Ett generellt gallringsbeslut finns för de handlingar som uppkommer under verksamhetsområde 1 (AN-04439/18). Förvaltningen har inte fattat tillämpningsbeslut på det generella gallringsbeslutet.

Nämndprotokoll och utskottsprotokoll bevaras. Protokollen diarieförs.

I Netpublicator Sign rensas handlingarna efter att den undertecknade handlingen diarieförts.

1.18 Sekretess (OSL och andra bestämmelser)

Innehåller behandlingen sekretessreglerade uppgifter?

Uppgifter kan vara reglerade i offentlighets- och sekretesslagen och därför extra skyddsvärda. Exempelvis en persons ekonomiska förhållanden.

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Utskottsprotokollen innehåller sekretessreglerade uppgifter enligt 25 och 26 kapitlet §1 offentlighets- och sekretesslagen och berör behandlingen myndighetsutövning mot enskild.

2 Personuppgifter, känslighet och behandlingens karaktär

2.1 Känsliga personuppgifter (art 9)

Behandlas känsliga personuppgifter?

Känsliga uppgifter är sådana uppgifter som kan skada en individs integritet i stor utsträckning om de görs tillgängliga, och som därför behöver extra skydd. Det är inte tillåtet att behandla känsliga uppgifter, förutom i undantagsfall. Känsliga personuppgifter kallas "särskilda kategorier av personuppgifter" i Dataskyddsförordningen.

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

2.1.1 Ange vilka känsliga personuppgifter som behandlas

☐ Etniskt ursprung
☒ Politiska åsikter
☐ Religiös eller filosofisk övertygelse
☐ Medlemskap i fackförening
☒ Hälsa
☐ Sexualliv eller sexuell läggning
☐ Genetiska uppgifter
☐ Biometriska uppgifter

2.1.2 Rättslig grund - känsliga (art 9)

Vilken eller vilka av följande rättsliga grunder gäller för behandlingen?

☐ Den registrerade har lämnat ett uttryckligt samtycke
☐ Skyldigheter inom arbetsrätt, social trygghet och socialt skydd
☐ Skyldigheter inom ramen för ett kollektivavtal
☐ Skydda någons grundläggande intressen (exempelvis livshotande)
☐ Behandlingen sker inom en ideell organisation[2]

[2] Undantaget gäller en Ideell organisation med politiskt, filosofiskt, religiöst eller fackligt syfte i relation till sina medlemmar, tidigare medlemmar och vissa andra personer som organisationen har regelbunden kontakt med relaterat till detta syftet (t ex kyrkobesökare, bidragsgivare och hjälpmottagare)

☒ En person har själv offentliggjort de känsliga uppgifterna
☐ Fastställa, göra gällande eller försvara rättsliga anspråk.
☒ Viktigt allmänt intresse
☐ Förebyggande hälso- och sjukvård och yrkesmedicin
☐ Bedömningen av en arbetstagares arbetskapacitet
☐ Kunna ställa medicinska diagnoser
☒ Tillhandahållande av hälso- och sjukvård eller behandling
☒ Social omsorg eller förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.
☐ Folkhälsoområdet (även förhindra smittspridning)
☒ Arkivändamål i allmänt intresse
☐ Forskningsändamål
☐ Statistiska ändamål
☐ Annat ändamål

Beskriv och kommentera ditt svar nedan:

Politiska åsikter är en känslig personuppgift enligt artikel 9 men eftersom förtroendevalda i nämnden för funktionsstöd själva har offentliggjort sin politiska tillhörighet så omfattas det av undantag.

Att en individ har insatser enligt SoL eller LSS är känsligt och detta framgår av utskottsprotokollen och berör behandlingen myndighetsutövning mot enskild.

2.2 Extra skyddsvärda personuppgifter

Inkluderar behandlingen någon av nedan kategorier av skyddsvärda uppgifter?

☒ Ja
☐ Nej

Om JA, Ange vilka typer av uppgifter som behandlingen omfattar:

☒ Inloggningsuppgifter
☐ Skyddad identitet
☐ Positioneringsdata
☒ Finansiella data
☐ Uppgifter om barn
☐ Löneuppgifter
☐ Uppgifter om lagöverträdelser
☐ Information som rör någons privata sfär
☐ Beteende och preferenser, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
☐ Uppgifter om sociala förhållanden
☐ Ej tillämpligt
☒ Annat

Beskriv och kommentera ditt svar nedan:

Personnummer, signeringspersonens bankinformation.

2.3 Beskrivning av användning av känsliga och/eller extra skyddsvärda PU

Ange i vilken omfattning som känsliga personuppgifter förekommer i behandlingen:

☒ I specifika fält
☒ I löpande text
☐ I begränsad omfattning
☐ I stor omfattning

Beskriv och kommentera ditt svar nedan:

I specifika fält vid signeringen förekommer personnummer samt signeringspersonens bankinformation. Cirka 24 protokoll per år.

Känsliga och/eller särskilt skyddsvärda uppgifter förekommer i löpande text i utskottsprotokollen och berör behandlingen myndighetsutövning mot enskild.

2.4 Utvärdering eller poängsättning

Inkluderar behandlingen utvärdering eller poängsättning?

Detta inbegriper att profilera eller förutsäga beteende, särskilt aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar.

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

2.5 Automatiskt beslutfattande

Inkluderar behandlingen användning av automatiskt beslutsfattande?

Behandling som har liten eller ingen påverkan på enskilda uppfyller inte detta särskilda kriterium.

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

2.6 Systematisk övervakning

Inkluderar behandlingen användning av systematisk övervakning?

Systematisk övervakning innebär att observera, övervaka eller kontrollera registrerade eller samla in i situationer där de registrerade kanske inte är medvetna om vem som samlar in deras uppgifter eller hur de kommer att användas.

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

2.7 Samkörning av uppgifter

Inkluderar behandlingen en samkörning av uppgifter från två eller flera behandlingar?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

2.8 Uppgifter om sårbara eller i beroendeställning

Inkluderar behandlingen sårbara individer eller personer i beroendeställning?

Innehåller behandlingen personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter.

☒ Anställda
☐ Barn
☒ Psykiskt sjuka personer
☐ Asylsökande – om det framgår
☐ Äldre personer
☐ Patienter
☐ Ej tillämpligt
☒ Andra

Beskriv och kommentera ditt svar nedan:

Brukare kan anses vara i en beroendeställning. Personuppgifterna hanteras i protokollen.

2.9 Ny teknik eller innovativa organisatoriska lösningar

Inkluderar behandlingen innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Digital signering har använts tidigare och är inget nytt i sig men osäkerhet kring bevarandet av handlingar och den digitala signaturen kan finnas då handlingar av denna typ inte funnits en längre tid.

2.10 Begränsning av rättigheter

Hindrar behandlingen registrerade från att utöva en rättighet, använda en tjänst eller ett avtal?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

3 Ansvarsskyldighet (efterlevnad av principer)

I detta avsnitt ska det beskrivas hur behandlingen tar hänsyn till de grundläggande principerna som finns för behandling av personuppgifter. Detta avsnitt syftar till att personuppgiftsansvarig ska kunna beskriva och visa hur den fullgör sin ansvarsskyldighet enligt art. 5.2 GDPR.

3.1 Laglighet (Ändamålsbegränsning)

Vilka åtgärder har utförts för att försäkra att insamlade uppgifter endast används för specifika, tydliga, och lagliga ändamål?

☒ Ändamålet för varje personuppgift identifieras innan insamlingen
☒ Det specifika ändamålet för varje personuppgift dokumenteras
☒ Personuppgifter samlas aldrig in enbart för att ”de är bra att ha”.
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

3.1.1 Ytterligare ändamål

För vilka ytterligare ändamål behandlas personuppgifter? Beskriv här om uppgifterna även kommer att användas inom någon annan verksamhet hos personuppgiftsansvarig.

☒ Arkivändamål av allmänt intresse
☐ Vetenskapliga forskningsändamål
☐ Historiska forskningsändamål
☐ Statistiska ändamål
☐ Inte säker

☐ Ej tillämpligt
☒ Annat

Om ytterligare behandlingar inte utförs, välj ”Ej tillämpligt”.

Beskriv och kommentera ditt svar nedan:

Systemet innehåller loggning av hur många digitala underskrifter som gjorts. Det går att se antalet inloggningar. Loggar sparas i 30 dagar.

Protokollen kommer i framtiden att levereras och bevaras hos Regionarkivet.

Underskrifter är kopplat till fakturering per licens och förvaltning gällande Netpublicator Sign. Kostnaden distribueras av Intraservice till de förvaltningar och bolag som använder tjänsten.

3.1.2 Automatiskt beslutfattande (rättslig grund)

Vilken av följande rättsliga grunder tillåter användning av data för automatiskt beslutsfattande?

(Hänvisning till fråga om automatiskt beslutsfattande ovan)

☐ Ingående eller fullgörande av ett avtal
☐ Beslutsfattandet tillåts enligt en lag som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen
☐ Den registrerades uttryckliga samtycke

Beskriv och kommentera ditt svar nedan:

Ej tillämpligt.

3.2 Korrekthet

Vilka åtgärder har utförts för att försäkra att behandlingen utförts korrekt (på ett juste/rättvist sätt)?

☒ Standardinställningar för användare är från början satt till högsta skydd
☒ Användare informeras om standardinställningarna och hur man ändrar dem
☐ Integritetsfunktioner, inställningar och relaterade funktioner är tydliga, framträdande, lättillgängliga och användarvänliga
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

En beställning läggs till Intraservice för att få behörigheten Mötes- och signeringsadministratör.

Mötes- och signeringsadministratör lägger beställning på användare och vilken behörighet/mapp de skall ha.

Mötes- och signeringsadministratör utgår från Intraservice rutin för Mötes- och signeringsadministratör.

Signerare läggs till manuellt av Mötes- och signeringsadministratör.

Förvaltningen för funktionsstöd kommer att ta fram rutin för signerare.

3.3 Öppenhet (transparens)

Får registrerade individer information om behandlingen?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Ordförare och justerare har informerats om tjänsten på presidiemöte, att deras personliga Bank ID kommer användas samt att det är frivilligt att signera digitalt, deras svar i frågan är nedtecknade i presidiets anteckningar. Tjänstepersoner har kännedom om att de förekommer i nämnd- och utskotts-protokollen.

När individer ansöker om bistånd ges information om dataskyddsförordningen vilka personuppgifter som samlas in, hur dessa hanteras samt information om deras rättigheter som registrerade. Ingen separat information ges om den digitala signeringen i Netpublicator Sign.

3.3.1 Kriterier för information

Uppfyller informationen till registrerade samtliga kriterier nedan?

☒ Koncis och transparant
☒ Begriplig och lättillgänglig
☒ Tydligt och enkelt språk
☒ Presenteras i skriftlig form eller på annat sätt
☒ Kostnadsfritt
☐ Inte säker
☐ Ej tillämpligt

Beskriv och kommentera ditt svar nedan:

Se avsnitt 3.3

3.3.2 Åtgärder för transparens

Vilka åtgärder har införts för att försäkra att uppgifterna är behandlade på ett transparent sätt?

☒ Användare får information om vem som samlar in/använder deras uppgifter
☒ Användare har möjlighet att rapportera problem/bekymmer
☒ Användare har tillgång till en inställningspanel/funktion för sekretess
☐ Visualisering med symboler används för att hjälpa till med tydlighet
☐ Information om integritet presenteras i lager eller flikar
☐ Certifiering, sigill och märkningar används för att visa transparens
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Se avsnitt 3.3

3.3.3 Samtycke

Valde du samtycke som laglig grund för behandlingen under *1.10 ovan*?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

3.3.3.1 Samtyckesförfrågan

Uppfyller samtyckesförfrågan samtliga kriterier?

☐ Skiljer sig tydligt från andra behandlingar i samma tjänst
☐ Begriplig och lättillgänglig
☐ Tydligt och enkelt språk

Beskriv och kommentera ditt svar nedan:

Ej tillämpligt

3.3.3.2 Samtycke – kriterier

Uppfyller samtycket samtliga kriterier nedan?

☐ Frivilligt givet
☐ Specifikt
☐ Den registrerade har blivit informerad
☐ Otvetydig

Beskriv och kommentera ditt svar nedan:

Ej tillämpligt

3.3.3.3 Samtycke – bevis

Bevaras bevis om samtycke för att kunna visa vad varje individ har gett samtycke för, vad de har fått för information, samt när och hur de gav sitt samtycke?

☐ Ja
☐ Nej
☐ Inte säker
☒ Ej tillämpligt

Beskriv och kommentera ditt svar nedan:

3.3.3.4 Samtycke – indragning

Är det lika lätt för individer att dra tillbaka sitt samtycke som det var att ge samtycket?

☐ Ja
☐ Nej
☐ Inte säker
☒ Ej tillämpligt

Beskriv och kommentera ditt svar nedan:

3.3.3.5 Samtycke – barn

Inhämtas föräldrars eller målsmans samtycke innan insamling av personuppgifter från ett barn under 13?

Notering: Detta gäller enbart för behandlingar relaterat till erbjudanden om samhällsinformationsservice (till exempel: e-handel, ISPs, sökmotorer, sociala medier etc.) som riktas direkt till ett barn.

☐ Ja
☐ Nej
☐ Inte säker
☒ Ej tillämpligt

Beskriv och kommentera ditt svar nedan:

3.4 Uppgiftsminimering

Vilka åtgärder har tagits för att försäkra att insamlingen är begränsad till uppgifter som enbart är lämpliga och relevanta för ändamålet?

☒ Verifikation sker på att tillräckliga och relevanta uppgifter samlas in
☒ Endast nödvändiga personuppgifter samlas in och sparas
☐ Dataöverföring begränsas till vad som är minimalt nödvändigt
☐ Rutiner för automatisk blockering och radering finns
☐ Frivilliga och obligatoriska fält är definierade i formulär
☐ Fritextfält styrs med tydlig policy
☐ Definierade fält (t.ex. färdiga svarsalternativ) används framför fritextfält
☐ Inte säker
☐ Ej tillämpligt
☒ Annat

Beskriv och kommentera ditt svar nedan:

I protokollen används endast relevanta personuppgifter, oftast begränsade till namn och personnummer. För varje protokoll skrivs uppgifter om vilka som ska justera in i modulen, dessa uppgifter sparas inte i modulen. Endast nödvändiga inloggningsuppgifter används.

3.5 Riktighet och kvalitet vid insamling

Vilka åtgärder har tagits för att säkerställa personuppgifternas kvalitet vid insamling?

☒ Individen lämnar själv uppgifterna och kan ändra vid behov
☒ Uppgifterna hämtas från Skatteverket eller liknande databas och anses vara korrekta
☐ Rutiner inkluderar regelbunden kontroll av att personuppgifter som insamlas är riktiga och håller god kvalitet
☐ Valideringskontroller för att upptäcka inkonsekvent, icke komplett, och felaktiga uppgifter
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Namn, personnummer och adresser hämtas centralt och förutsätts vara korrekta. (Troman, ett kommungemensamt system kopplat till folkbokföringen).

Uppgifter om bankinformation förekommer.

3.6 Riktighet och kvalitet – löpande

Vilka åtgärder har vidtagits för att säkerställa att uppgifter kontinuerligt är riktiga och uppdaterade?

☒ Individen lämnar själv uppgifterna och kan ändra vid behov
☒ Uppgifterna uppdateras från Skatteverket eller liknande databas och anses vara korrekta
☐ Löpande kontroller av personuppgifters riktighet och kvalitet
☐ Valideringskontroller för att filtrera ut gamla personuppgifter
☐ Gamla personuppgifter raderas eller uppdateras
☐ Inte säker
☐ Ej tillämpligt
☒ Annat

Beskriv och kommentera ditt svar nedan:

Se avsnitt 3.5

3.7 Lagringsminimering

Vilka åtgärder har du tagit för att försäkra att personuppgifter inte lagras längre än nödvändigt?

En dokumenthanteringsplan och gallringsbeslut avgör när, om och hur handlingar får gallras. En hänvisning till dokumenthanteringsplanen finns *under 1.17 Lagring (Dokumenthanteringsplan).* Frågan nedan rör hur gallringsbeslut är implementerade.

Notera: I många fall behöver uppgifter sparas längre beroende på allmänt intressen, forsknings- eller historisk synpunkt, eller för statistiska ändamål.

☒ Processer finns för granskning och gallring av personuppgifter
☐ Kriterier med trigger är implementerade och radering sker systematiskt
☒ Personuppgifter begränsas eller raderas när en registrerad är inaktuell
☐ Inte säker
☐ Ej tillämpligt
☒ Annat

Beskriv och kommentera ditt svar nedan:

Protokollen i sin helhet diarieförs och bevaras för alltid.

Inom Netpublicator Sign rensas handlingarna efter att den undertecknade handlingen diarieförts.

3.8 Integritet och konfidentialitet

3.8.1 Klassning

Har ni informationssäkerhetsklassat behandlingen?

☒ Ja
☐ Nej

Behandlingen ska klassas utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet, i enlighet med den organisationsövergripande klassningsmodellen. Ange alltså vilken informationssäkerhetsklassning som behandlingen har och inte informationsbärarens/systemets säkerhetsklassning. Värdena 0, 1 eller 2 ska anges för respektive fält nedan.

Värdera behandlingens Konfidentialitet (K)
☐ 0 ☐ 1 ☒ 2

Värdera behandlingens Riktighet (R)
☐ 0 ☐ 1 ☒ 2

Värdera behandlingens Tillgänglighet (T)
☐ 0 ☒ 1 ☐ 2

Beskriv eller kommentera klassningen:

Klassificeringsmallen från 2021-10-01 har använts.

3.9 Proportionalitet och nödvändighet

Proportionalitet och nödvändighet innebär att behandlingen och dess eventuella inskränkningar i den enskildes personliga integritet – med hänsyn till skyddsåtgärder – är proportionell mot det eftersträvade syftet och att de registrerades grundläggande rättigheter och intressen säkerställs.

3.9.1 Proportionell (nytta minus risker)

Är nyttan med behandlingen proportionell mot de nackdelar, risker och problem som behandlingen leder till eller kan leda till för enskildas personliga integritet?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Bara den information som krävs för behandlingen används. Ur rättssäkerhetssynpunkt skapas möjlighet till skyndsam och effektiv hantering av politisk ärendehantering.

Det är även ett säkerställande att den politiska ärendehanteringen kan fortgå oavsett oförutsedda händelser som förhindrar de förtroendevalda från att infinna sig fysiskt för analog signering, som exempelvis skedde under Covid-19 pandemin.

Intrånget i den personliga integriteten som det innebär för förtroendevalda och nämndsekreterare att uppge sitt personnummer och BankID är att anse som försumbart i jämförelse med de nyttor i form av effektivitet och kontinuitet som uppnås med digital signering.

3.9.2 Nödvändig

Finns det ett annat sätt att uppnå samma resultat?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Samma information hanteras som i den manuella hanteringen. Nyttan av att snabbt kunna signera överväger den risk som finns med det görs digitalt. Elektroniska underskrifter kan minska smittorisker. Tidsvinster vid brådskande signering bör också vägas in till behandlingens fördel.

3.9.3 Bedömning intresseavvägning

Valde du intresseavvägning som svar på rättslig grund under *1.10 ovan*?

☐ Ja
☒ Nej

Nej är förvalt. *En myndighet kan inte använda intresseavvägning i sin myndighetsutövning. Istället används* ***allmänt intresse*** *vid exempelvis hantering av anställdas information eller behandlingar som sker säkerhetsändamål.*

3.9.4 Om Intresseavvägning (berättigat intresse)

Vilket är det berättigade intresset för den personuppgiftsansvarige?

☐ Direktmarknadsföring
☐ Förhindrande av bedrägeri, missbruk eller penningtvätt
☐ Dela data om anställda inom organisationen för interna administrativa syften
☐ Dela data om kunder inom organisationen för interna administrativa syften
☐ System för att slå larm om missförhållanden (whistleblowing)
☐ Övervakning av anställda i säkerhets- och riskhanteringssyfte
☐ Verkställande av rättsliga krav inklusive indrivning genom förfaranden utanför domstol
☐ Fysisk säkerhet, IT-säkerhet och nätverkssäkerhet

☐ Behandling för historiska, vetenskapliga eller statistiska ändamål
☐ Behandling för forskningsändamål (inklusive marknadsundersökningar)
☐ Fysisk säkerhet, IT-säkerhet och nätverkssäkerhet
☐ Annat

Beskriv och kommentera ditt svar nedan:

Ej tillämpligt.

3.9.5 Om Intresseavvägning (berättigat intresse) - Analys

Vänligen förklara varför det berättigade intresset hos personuppgiftsansvarig väger tyngre än intressen eller grundläggande fri- och rättigheter hos individer.

Ej tillämpligt.

4 Individers rättigheter

4.1 Tillämpliga rättigheter

I artiklarna 12-21 GDPR finns det rättigheter för den enskilde. Vilka artiklar blir aktuella av den aktuella behandlingen?

☒ Art. 12 – Informationspolicy om hur personuppgifter behandlas
☒ Art. 13 – Informationsskyldighet när enskild lämnat uppgiften
☒ Art. 14 - Informationsskyldighet när annan än enskild lämnat uppgiften
☒ Art. 15 – Registerutdrag
☒ Art. 16 – Rättelse
☒ Art. 17 – Radering
☒ Art. 18 – Begränsning av behandling
☒ Art. 19 – Anmälningsskyldighet till mottagare
☐ Art. 20 – Dataportabilitet
☒ Art. 21 – Invändning

Beskriv och kommentera ditt svar nedan:

4.2 Administrativa åtgärder för rättigheter

Beskriv vilka administrativa åtgärder har bedömts behövas för att säkerställa att de registrerades rättigheter tillvaratas.

Interna rutiner för tjänstepersoner och politiker om hur man använder systemet och om lagring och rensning av handlingar finns.

Brukares uppgifter behandlas endast tillfälligt i Netpublicator Sign, det är en mycket kort tidsperiod i samband med registreringen. Rutiner finns för hantering av rättelse, personuppgiftsincident. Information om hur personuppgifter behandlas lämnas på Goteborg.se samt vid den tidpunkt då en individ ansöker om bistånd. Inte sannolikt att rättigheterna kommer att aktualiseras eftersom det inte är en lagringsplats. Däremot kan tjänstepersoners och förtroendevaldas rättigheter komma i fråga och i så fall handlar det om roll, kontaktuppgifter, personnummer och inloggningsuppgifter.

4.3 Tekniska åtgärder för rättigheter (PbD)

Beskriv vilka tekniska åtgärder som behöver vara inbyggda i systemet/tjänsten för att säkerställa att de registrerades rättigheter tillvaratas.

Det går att söka fram användare och deras uppgifter i systemet och exportera dessa uppgifter. Signerare måste tas fram manuellt per förvaltning. Det går inte att söka fram andra signerare för andra förvaltningar. Dokument försvinner när det är signerat för signerare. Manuell rutin finns för mötesadministratören när protokollet är signerat, diarieför protokollet och därefter tar bort det från Netpublicator sign.

4.3.1 Personuppgiftsansvarig och personuppgiftsbiträdet?

Beskriv vilka tekniska åtgärder som har bedömts behövas mellan personuppgiftsansvarig och personuppgiftsbiträdet för att de registrerades rättigheter ska tillvaratas.

Avtal gällande kommungemensamma tjänster GBG Stad.

5 Tredjelandöverföring

5.1 Förekomst

Överförs personuppgifter till tredjeland eller internationell organisation?

Det finns strikta regler i dataskyddslagstiftningen för när personuppgifter får lämnas till länder utanför EU/EES, så kallat tredjeland. Detta gäller all överföring, även till personuppgiftsbiträden som inte själva använder personuppgifterna i sin verksamhet utan bara lagrar, driftar, supportar, utvecklar, underhåller eller servar systemet. Observera att ordet överföring även omfattar åtkomst till personuppgifterna i tredjeland, även om de lagras inom EU/EES.

☐ Ja
☒ Nej

5.1.1 Ange vilket tredjeland och mottagare

Mottagaren kan vara en extern verksamhet eller ett företag inom koncernen som finns utanför EU/EES. Vem mottagaren är kan vara av intresse bland annat för vilka avtal som ska ingås. Exempel: "Biträde X i USA", "Intern verksamhet Y i Japan", "Internationell organisation Z".

Ej tillämpligt.

5.2 Grund för tredjelandsöverföring

På vilka grunder sker överföringen till tredjeland eller internationell organisation?

☐ EU-kommissionens standardavtal överenskommelse om transatlantisk dataöverföring (Privacy shield)
☐ Bindande företagsbestämmelser (Binding Corporate Rules, BCR)
☐ EU-kommissionen har godkänt mottagandet som har ansetts ha en godkänd skyddsnivå
☐ Godkänd certifieringsmekanism
☐ Godkänd uppförandekod
☐ Eget avtal mellan parterna som godkänts av tillsynsmyndigheten
☐ Viktigt allmänintresse
☐ Avtal med den registrerade
☐ Rättsliga anspråk
☐ Samtycke
☐ Annat

Beskriv och kommentera ditt svar nedan:

Ej tillämpligt.

6 Personuppgiftsbiträden (PUB)

6.1 Extern drift

Sköts delar av driften av behandlingen externt för informationsbärare (system)?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Intraservice.

6.2 Omfattning

Anlitas personuppgiftsbiträde för hela eller delar av behandlingen?

☒ Ja
☐ Nej

Om Ja beskriv kort i vilka delar av behandlingen.

6.3 Personuppgiftsbiträdesavtal (PUB-avtal)

Bifoga det avtal alt. det förslag som finns mellan personuppgiftsansvarig och personuppgiftsbiträdet.

Personuppgiftsbiträdesavtal mellan Netpublicator Apps och Intraservice Diarienummer 0199/17. Avtal mellan PUA och Intraservice i rollen PUB hittas i generella regler för kommungemensamma interna tjänster Diarienummer 0014/18 (0110/20). Bilaga 1 bifogas.

6.4 Instruktioner

Bifoga de instruktioner alt. det förslag som finns mellan personuppgiftsansvarig och personuppgiftsbiträdet.

Bilaga 2 bifogas.

6.5 Leverantörskontroll

Har en leverantörskontroll genomförts för att granska leverantörens efterlevnad av informationssäkerhet och dataskydd?

En rutin för leverantörskontroll beskrivs i dokumentet *Rutin – Processbeskrivning - efterlevnadskontroll av leverantör.*

☒ Ja
☐ Nej

Efterlevandekontroll genomfört 2021 av Intraservice enligt rutin.

Beskriv och kommentera ditt svar nedan:

6.6 Har PUB egna syften?

Beskriv om personuppgiftsbiträdet avser att behandla uppgifterna för något eget syfte, både som rådata, eller efter anonymisering av personuppgifterna.

Nej.

6.7 Underbiträde

Har PUB redovisat vilka underbiträdesavtal som är tecknade?

☒ Ja
☐ Nej

7 Delning

7.1 Utlämnande till tredje part

Lämnas några personuppgifter ut till tredje part?

☐ Ja
☒ Nej

Om Ja, Ange mottagare:

7.2 Informationsskyldighet (lag, förordning eller föreskrift)

Finns det någon skyldighet för personuppgiftsansvarig att lämna uppgifter till någon annan myndighet eller organisation enligt lag, förordning eller föreskrift?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Netpublicator Sign är ingen lagringsplats. Utlämnande sker därmed aldrig direkt från Netpublicator Sign.

7.2.1 Elektroniskt utlämnande

Om det finns en skyldighet att lämna personuppgifter till någon annan kommer detta ske elektroniskt?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Ej tillämpligt.

8 Övrigt

8.1 Certifieringar eller uppförandekoder[3]

Känner du till några godkända certifieringar eller branschspecifika uppförandekoder som leverantören följer? (Code of conduct)

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

9 Risker och åtgärder

En riskbedömning genomförs och dokumenteras i en bilaga (Excel eller annat dokument)

Infoga riskdokument:

Se bilaga 5. Riskanalysen är gemensam för båda behandlingarna då det inom de båda behandlingarna hanteras känsliga personuppgifter och bedömningen i huvudsak är identisk. Om risken avser en av behandlingarna tydliggörs det i den punkten i riskanalysen.

[3] Certifieringar och branschspecifika uppförandekoder är utarbetade av organisationer eller andra representativa organ och är giltiga om de är godkända av en tillsynsmyndighet i EU, europeiska dataskyddsnämnden (EDPB) eller EU-kommissionen för att uppfylla GDPR-efterlevnad.

9.1 Sammanfattning av riskbedömning

Nedan är de risker med högst riskvärde efter åtgärd. För en komplett förteckning av identifierade risker så kan en komplett riskbedömning i Excel biläggas rapporten

#	Benämning	Beskrivning	Konsekvens	avser	Sannolikhet	Riskvärde
R14	Feltaggad information	Information blir feltaggad genom att den skickas med fel mall. Mottagare kan därför få tillgång till känslig information längre än nödvändigt utan att vara medveten om det. Pga mänskliga faktorn, okunskap.	*4*	☒ röjande ☐ ändring ☐ förlust	*2*	*8*
R21	Handlingar lämnas i Netpublicator	Handlingar har inte raderats korrekt pga Handhavandefel, okunskap. Gäller både i Netpublicator Sign och lokalt i mellanlagret.	*4*	☒ röjande ☐ ändring ☒ förlust	*2*	*8*
R27	Incidenter upptäcks inte	Personuppgiftsincidenter upptäck inte i tid eller inte alls. Pga att Incidenthantering saknas, svårt att upptäcka, okunskap, incident rapporteras inte.	*4*	☒ röjande ☐ ändring ☒ förlust	*2*	*8*

9.2 Riskidentifiering

Riskerar den registrerade att utsättas för någon eller några av följande skador som orsakats av behandlingen eller som konsekvens av en personuppgiftsincident?

☐ Diskriminering
☒ Identitetsstöld
☐ Bedrägeri
☐ Ekonomisk förlust
☒ Påverkan på rykte
☒ Förlust av konfidentialitet
☒ Anonymisering röjs av obehörig
☐ Betydande påverkan på det ekonomiska och sociala förhållandet
☒ Förlust av mänskliga fri- och rättigheter
☐ Förhindra individers kontroll över sina uppgifter
☐ Sannolikt sker ingen skada till följd av behandlingen
☐ Inte säker
☐ Ej tillämpligt

☐ Annat

Beskriv och kommentera ditt svar nedan:

9.3 Riskkällor

Vilka potentiella källor finns som kan orsaka dessa skador?

☒ Dataintrång
☒ Antagonist
☐ Kriminalitet
☐ Bristande övervakning
☒ Bristfällig policy/tillvägagångsätt
☐ Oskyddad lagring
☐ Brist på ansvarsskyldighet
☒ Brist på experter inom ämnet/ämneskompetens
☐ Otillräcklig testning
☒ Otillräcklig utbildning/övning/träning
☐ Driftstörning, haveri
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

9.4 Riskgrupper

Vilka specifika grupper av individer risker att skadas?

☒ Kunder/användare
☐ Entreprenörer
☒ Anställda
☐ Arbetssökande
☐ Asylsökande
☐ Patienter
☐ Besökare
☐ Studenter
☐ Inte säker
☐ Ej tillämpligt
☒ Annat

Beskriv och kommentera ditt svar nedan:

Politiker och de som kan komma att omfattas av ett beslut i nämnd eller utskott.

9.5 Riskperspektiv

Hur kan dessa potentiella skador uppfattas av de registrerade?

Det kommer att finnas möjlighet till en manuell hantering. Skulle ett beslut felaktigt signeras går det att rätta till eftersom beslutsunderlag från tidigare del i processen kommer att finnas tillgängligt. Den registrerade kan antas uppfatta riskerna som acceptabla efter införda åtgärder.

Om detta inte kan förutses, bör en de registrerades tillfrågas för att ge sin uppfattning om behandlingen

9.6 Tekniska säkerhetsåtgärder

10 Vilka tekniska åtgärder har införts för att minska de risker som identifierats under *9 Risker och åtgärder*Individers rättigheter

10.1 Tillämpliga rättigheter

I artiklarna 12-21 GDPR finns det rättigheter för den enskilde. Vilka artiklar blir aktuella av den aktuella behandlingen?

☒ Art. 12 – Informationspolicy om hur personuppgifter behandlas
☒ Art. 13 – Informationsskyldighet när enskild lämnat uppgiften
☒ Art. 14 - Informationsskyldighet när annan än enskild lämnat uppgiften
☒ Art. 15 – Registerutdrag
☒ Art. 16 – Rättelse
☒ Art. 17 – Radering
☒ Art. 18 – Begränsning av behandling
☒ Art. 19 – Anmälningsskyldighet till mottagare
☐ Art. 20 – Dataportabilitet
☒ Art. 21 – Invändning

Beskriv och kommentera ditt svar nedan:

ovan?

☒ Autentisering
☒ Anti-malware

☐ Detekteringsverktyg för personuppgiftsincidenter (Data Breach)
☒ Säkerhetskopiering (backup)
☐ Kryptering
☐ Brandväggar
☐ Detekteringsverktyg för intrång
☒ Loggning
☒ Logisk kontroll av åtkomst
☒ Flerfaktorsautentisering
☐ Nätverksautentisering
☐ Pseudonymisering (Anonymisering)
☐ Regelbundna mjukvaruuppdateringar (Patchning)
☐ Detekteringsverktyg för sårbarheter
☐ Mobile device management (MDM)
☐ Inte säker
☐ Ej tillämpligt
☒ Annat

Beskriv eller kommentera vilka administrativa skyddsåtgärder som behövs för att säkerställa en lämplig säkerhetsnivå:

Datahalls-säkerhet. Att risk för personuppgiftsincidenter minimeras i samband med utveckling av applikationen och i Intraservice arbete med att leverera tjänsten.

10.2 Administrativa åtgärder

11 Vilka administrativa åtgärder har genomförts för att hantera de risker som identifierats under *9 Risker och åtgärder*Individers rättigheter

11.1 Tillämpliga rättigheter

I artiklarna 12-21 GDPR finns det rättigheter för den enskilde. Vilka artiklar blir aktuella av den aktuella behandlingen?

☒ Art. 12 – Informationspolicy om hur personuppgifter behandlas
☒ Art. 13 – Informationsskyldighet när enskild lämnat uppgiften
☒ Art. 14 - Informationsskyldighet när annan än enskild lämnat uppgiften
☒ Art. 15 – Registerutdrag
☒ Art. 16 – Rättelse
☒ Art. 17 – Radering
☒ Art. 18 – Begränsning av behandling
☒ Art. 19 – Anmälningsskyldighet till mottagare
☐ Art. 20 – Dataportabilitet

☒ Art. 21 – Invändning

Beskriv och kommentera ditt svar nedan:

ovan?

☒ Riktlinjer för datoranvändning
☒ Utbildning och informationsinsatser
☒ Kontinuitetsplan
☒ Incidenthanteringsplan
☒ Katastrofberedskap (Disaster recovery plan)
☒ Behovsenlig behörighet (Need-to-know)
☒ Sekretessavtal
☐ Lösenordspolicy
☐ Penetrationstestning
☒ Säkra lokaler
☐ Tillsyn/interna kontroller
☐ Övervakning
☐ Simulerings- och krisövningar
☐ Bakgrundskontroller
☒ Säker radering
☒ Åtkomstkontroll
☒ Personuppgiftsbiträdesavtal
☒ Leverantörskontroller
☐ Inte säker
☐ Ej tillämpligt
☒ Annat

Beskriv eller kommentera vilka administrativa skyddsåtgärder som behövs för att säkerställa en lämplig säkerhetsnivå:

Tydliga instruktioner i PUB-avtal enligt förslag i riskanalysen (se bilaga Net-publicator sign komplett riskanalys). Tydliga instruktioner av handhavande finns tillgängliga för de som ska genomföra digital signering.

11.2 Inbyggt dataskydd – Privacy by Design (art 25, 26)

Beskriv hur behandlingen tar hänsyn till principen om inbyggt dataskydd i artiklarna 25 och 26?

Inbyggt dataskydd och dataskydd som standard med mål att säkerställa att processer och system är utformade så att inhämtande och behandling (inklusive användning, utlämnande, bevarande, överföring och radering) begränsas till det som är nödvändigt för det identifierade ändamålet.

Rollbaserad behörighetsstyrning används i systemet. I övrigt är det osannolikt att Privacy by Design är applicerbart på systemet eftersom det inte är en lagringsplats. Systemet/applikationen är inte heller konstruerad för att dela information med andra.

11.3 Bedömning kvarvarande risk

Är de identifierade planerade åtgärderna som föreslås tillräckliga för att minska de identifierade riskerna till en nivå så att behandlingen *inte sannolikt leder till en hög risk för fysiska personers fri- och rättigheter*?

☒ Ja
☐ Nej

11.4 Förhandssamråd

Vid nej ovan så är den kvarvarande risken hög och Datainspektionen bör rådfrågas (artikel 36.1). För det fall ni inte lyckas avhjälpa alla allvarliga risker behöver ni söka förhandssamråd hos Datainspektionen innan behandlingen kan påbörjas. För förhandssamråd kräver Datainspektionen att verksamheten gjort en konsekvensbedömning och arbetat med riskminimering.

Har eller kommer ni begära förhandssamråd hos Datainspektionen?

☐ Ja
☒ Nej

Om Nej, motivera:

De planerade åtgärder (som redovisas i bilaga Netpublicator Sign komplett riskanalys) minskar de identifierade riskerna till en sådan nivå att behandlingen inte sannolikt leder till en hög risk för fysiska personers fri- och rättigheter.

12 Bilagor

Här kan du ange om det utöver denna rapport finns ytterligare handlingar som har legat till grund för bedömningarna samt de handlingar som blir bilagor till denna rapport.

☐ Beskrivning av verksamhet,

☐ Beskrivning av IT-system och/eller IT-säkerhet,

☒ Riskanalys,

Se bilaga 5.

☒ Personuppgiftsbiträdesavtal,

Se bilaga 1.

☐ Underlag till PUA,

☒ Intraservice riskbedömning,

Se bilaga 6.

☒ Annat:

Se bilaga 2 och 3.

☐ Specifika säkerhetsåtgärder:

13 Referenser

Artikel 29-gruppen (2017) WP 248 rev. 01, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 4 april 2017, senast reviderade och antagna den 4 oktober 2017 Länk

Artikel 29-gruppen (2018) WP251rev.01 Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, antagna den 3 oktober 2017, senast reviderade och antagna den 6 februari 2018

Artikel 29-gruppen (2018) WP260rev.01 Riktlinjer om öppenhet enligt förordning (EU) 2016/679 Antagna den 29 november 2017, senast granskade och antagna den 11 april 2018

Artikel 29-gruppen (2013) WP 203 Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013

Artikel 29-gruppen (2014) WP 217, Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, antaget den 9 april 2014

CNIL Commission Nationale de l'Informatique et des Libertés (2018) *Privacy Impact Assessment (PIA) 3 : knowledge bases* Länk

Datainspektionens hemsida om konsekvensbedömning. Länk

European Data Protection Supervicer (EDPS) (2019) *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation,* v1.3 July 2019 Länk

International Standard Organisation -ISO (2017) *ISO/IEC 29134:2017 1 Information technology -- Security techniques -- Guidelines for privacy impact assessment.* Länk

14 Appendix 1 – Exempel på konsekvenser och sannolikheter

14.1 Konsekvenser [4]

Konsekvens-nivå	Generisk beskrivning	Exempel på skada		
		Fysisk	**Materiell**	**Moralisk**
1. Försumbar	Registrerade är inte påverkade eller har små besvär, som de kan komma över utan problem. T.ex personuppgifter som är allmänt tillgänglig (t.ex. i telefonböcker, adressböcker eller listor)	• Bristande omvårdnad (barn, en person beroende av hjälp) • Huvudvärk	• Tidsförlust på grund av formaliteter • Spam • Direktmarknadsföring • Riktad annonsering som konsument	• Ren skär irritation • Rädsla att tappa data • Känsla av obehag av närgångenhet • Smärre tidsförlust • Bristande respekt • Missade erbjudanden
2. Måttlig	Registrerade kan påverkas med tydliga besvär, som de kan komma över, trots vissa svårigheter. T.ex personuppgifter som kräver ett legitimt intresse för åtkomst (t.ex. begränsade offentliga filer eller medlemmarna i en distributionslista)	• Mindre fysisk påverkan (illamående, ångest) • Bristande omvårdnad som orsakar skada • Förtal som resulterar i psykisk eller fysiska symptom.	• Oväntade kostnader (böter, avgifter) • Ej access till tjänster • Missade möjligheter (karriär, semester) • Oönskad post som orsakar skada • Kostnadsökningar • Inkorrekt profilering • Exponering av hemliga uppgifter (graviditet, rehabilitering)	• Avstängning från en tjänst • Ärekränkning och försämrat rykte • Problem med professionella eller personliga relationer (bilder, skamfilning) • Känsla av intrång i privatlivet • Förolämpning på sociala medier
3. Allvarlig	Registrerade påverkas med betydande besvär, som de bör kunna komma över med mycket svårigheter och hjälp. T.ex personuppgifter vars obehöriga avslöjande kan påverka den registrerades rykte (t.ex. information om inkomst, socialförsäkringsförmåner, fastighetsskatt eller påföljder)	• Allvarlig fysisk påverkan som orsakar långsiktiga problem. • Handikapp och fysisk förändring som ett resultat av våld, olycka hemma eller på arbetet	• Bestående ekonomiska problem (måste låna) • Ej möjlighet att låna • Förlust av bostad, arbete, egendom • Separation • Finansiell förlust på grund av bedrägeri • Frysning av tillgångar • Nekad att studera, examen, utvisning	• Allvarliga psykiska problem (depression, fobier) • Känsla av intrång med bestående skada • Kränkning av grundläggande rättigheter (diskriminering, åsiktsfrihet) • Utpressning • Nätmobbning & trakasserier • Maktlöshet av att förlorat en process
4 Mycket allvarlig	Registrerade påverkas med allvarliga besvär, eller oöverstigliga konsekvenser, som kanske inte kan komma över. T.ex personuppgifter vars obehöriga avslöjande, modifiering, förlust eller förstörelse kan påverka den registrerades existens eller hälsa, frihet och liv.	• Långsiktig påverkan med permanenta eller kronisk fysiska besvär • Död (mord, självmord, olycka) • Permanent funktionsnedsättning	• Förlust av bevis (rättsprocess) • Oförmåga att arbeta • Ej möjligt att flytta • Förlust av vital infrastruktur (vatten, el)	• Långsiktig eller permanent psykisk påverkan • Kriminell bestraffning • Förlust av familjeband • Förlust av myndighet eller förmyndarskap • Ej möjlighet att föra process

[4] Enligt CNIL (Franska Tillsynsmyndigheten) Privacy Impact Assessment (PIA) samt ISO 29134 råd för konsekvensbedömning (Privacy impact assessment)

14.2 Sannolikhet

Sannolikheten för att varje hot utnyttjas bör uppskattas med hänsyn till sårbarheterna för behandlingar och deras stödsystem och kapaciteten hos riskkällor för att utnyttja dem (färdigheter, tillgänglig tid, ekonomiska resurser, närhet till informationssystem, motivation, känsla av straffrihet, etc.). Med andra ord, i vilken utsträckning kan egenskaperna för underlättande tillgångar utnyttjas för att utföra ett hot?

Osannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar inte möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i ett rum som skyddas av en kortläsare och åtkomstkod).

Möjlig: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara svårt för de valda riskkällorna (t.ex. stöld av pappersdokument som är lagrade i ett rum skyddat av en kortläsare).

Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade på kontor som inte kan nås utan att först kontrollera i receptionen).

Mycket Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara extremt lätt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i en lobby).

15 Appendix 2 – Lista på personuppgiftskategorier

Kategori	Exempel på personuppgifter
Anställningsinformation	• Uppgifter om anställningsförmåner • Anställningsnummer • Företagskredit- eller betalkortsnummer • Anspråk om ersättning till anställda • Jobbtitel/roll • Disciplinär åtgärd • Frånvaroregister/tidsspårning/årlig ledighet • Hälso- och säkerhetsrelaterad information och rapportering • Slutdatum och skäl för uppsägning • Tidigare arbetslivserfarenhet • Arbetstimmar • Avtalstyp - bestämd tidsperiod / tillfällig / fast anställning, etc. • Prestationsbedömning • Lön • Startdatum • Avgångsintervju och kommentarer • Detaljer om jobbansökan (t.ex. ansökningsblankett, intervjuanteckningar, referenser) • Överordnad chef • Klagomål • Kontorsadress • Verksamhet/Enhet • Personalnummer
Arbetsmiljö	• Detaljer om mobbning och trakasserier
Bakgrundskontroller	• Drogtestresultat • Referens- eller bakgrundskontroller • Belastningsregister • Trafikböter • Brottshistorik
Biometriska och genetiska uppgifter	• Näthinneskanning • Ansiktsigenkänning • Röstigenkänning • Fingeravtryck • Genetisk sekvens
Inloggningsuppgifter	• Kontonummer • Kontoålder • Kontolösenord
Familjeinformation	• Namn på föräldrar • Namn på barn • Namn på partner • Annan familjestatus & information om närstående
Finansiella uppgifter	• Bankkontoinformation • Kontoutdrag • Bonusutbetalningar • Kreditkortsnummer • Ersättningsuppgifter • Uppgifter om lån, krediter, amorteringar etc

	• Finansiell status (inkomst, egendomar, investeringar)
Kontaktinformation	• Tidigare bostadsadress • Hemadress • Kontaktuppgifter vid nödfall • Telefonnummer • Personlig e-postadress • Kontaktuppgifter
Myndighetsutfärdad identifikation	• Personnummer • Körkortsnummer • Detaljer om nationellt identitetskort • E-tjänstekort • Pass • ID-kort • Skyddad identitet
Personlig identifikation	• Förnamn • Efternamn • Vikt • Födelsedatum • Religion/Religiös övertygelse • Sexuell läggning • Längd • Fullständigt namn • Civilstånd • Signatur • Ras eller etniskt ursprung • Nationalitet • Kön • Hälsa • Ålder • Foto, bild • Alias eller pseudonymer • Kännetecken
Resor och kostnader	• Resehistorik • Resebokningsinformation • Uppgifter om kostnader
Sociala välfärdsdata	• Arbetslöshetsersättning • Förtidspension • Försörjningsstöd eller andra bistånd (utsatthet, arbetslöshet, fattigdom)
Sociala medier	• Sociala medier - konto • Sociala medier - historik • Sociala medier - kontaktuppgifter
Personliga egenskaper, utbildning och arbete	• Examensbevis • Betyg • Utbildningshistorik • Språk • Akademiska meriter • Förbundsmedlemskap • Kvalifikationer/certifieringar • Curriculum vitae • Utvärderingsinformation • Fackligt medlemskap • Beteende och preferenser • Vanor, personliga preferenser & intressen, umgängesliv & kontakter

	• Utvärderingar av personlighet och beteende
Tekniska metadata	• Webbplatshistorik • Lokaliseringsdata (Position) • Cookie-information • IP-adress • Webbsökningstid • Trafikdata • Information om använda telefontjänster (Har ringt 1177 t.ex.) • Loggar (applikationsloggar, säkerhetsloggar etc.)