BILAGA 3: PERSONUPPGIFTSBITRÄDESAVTAL

1 BAKGRUND

1.1 Kivra kommer att behandla personuppgifter i syfte att tillhandahålla Tjänsterna som följer av de Allmänna Villkoren som ingåtts mellan Parterna. Detta personuppgiftsbiträdesavtal ("**Personuppgiftsbiträdesavtal**") reglerar förhållandet mellan Kivra och Avsändaren där Kivra agerar i egenskap av personuppgiftsbiträde och Avsändaren i egenskap av personuppgiftsansvarig.

1.2 Om och i den mån annat bolag i samma koncern som Avsändaren är att betrakta som personuppgiftsansvarig (ensamt eller tillsammans med Avsändaren) för behandling som omfattas av detta Personuppgiftsbiträdesavtal, bekräftar Avsändaren härmed att man inhämtat nödvändiga tillstånd för att ingå Personuppgiftsbiträdesavtalet även för sådant bolags räkning.

1.3 Om det finns motsägelse mellan de villkor som anges i detta Personuppgiftsbiträdesavtal och andra avtal, dokument eller instruktioner, oavsett form, som rör behandlingen av personuppgifter, ska villkoren i detta Personuppgiftsbiträdesavtal ha företräde och vara styrande för Parternas åtaganden och handlingar med avseende på personuppgiftsbehandling.

2 DEFINITIONER

2.1 De definitioner och termer som används i detta Personuppgiftsbiträdesavtal ska ha samma betydelse och innebörd som de definitioner och termer som anges i de Allmänna Villkoren.

2.2 Följande begrepp ska ha nedan angiven betydelse om inte omständigheterna tydligt föranleder något annat (och termer som inte är definierade i Personuppgiftsbiträdesavtalet såsom t.ex. ”personuppgiftsansvarig”, ”personuppgiftsbiträde”, ”personuppgift”, ”behandling”, ”personuppgiftsincident” ska ha den betydelse som framgår av Dataskyddsförordningen):

”**Dataskyddsförordningen**” avser Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

”**Registrerad**” avser en fysisk person vars personuppgifter ingår i Uppgifterna.

”**Tillämplig Dataskyddslagstiftning**” avser: (i) Dataskyddsförordningen och ersättande rättsakter; (ii) tillämplig svensk lag avseende dataskydd; och (iii) till i) och ii) hörande förordningar och föreskrifter som utfärdats av Tillsynsmyndighet och som är tillämpliga på Parts verksamhet.

”**Tillsynsmyndighet**” avser Integritetsskyddsmyndigheten och i förekommande fall annan behörig tillsynsmyndighet som med stöd av lag utövar tillsyn över Parts verksamhet.

”**Uppgifterna**” avser de personuppgifter som överförs till, lagras eller på annat sätt behandlas av Kivra på uppdrag av Avsändaren enligt detta Personuppgiftsbiträdesavtal. Vilka typer av personuppgifter som omfattas anges i Underbilaga A till detta Personuppgiftsbiträdesavtal.

3 INSTRUKTIONER

3.1 Personuppgiftsbiträdesavtalet består av detta dokument, Underbilaga A och Underbilaga B. I Underbilaga A finns en specifikation över behandlingen och i Underbilaga B beskrivs Kivras säkerhetsåtgärder.

3.2 Avsändaren ger Kivra tillstånd att överföra Uppgifterna till tredje part i de fall som krävs för att uppfylla syftet med detta Personuppgiftsbiträdesavtal, inbegripet dess instruktioner, och/eller för att uppfylla en rättslig förpliktelse. Detta inkluderar, men är inte begränsat till, överföring av Uppgifterna till leverantörer, samarbetspartners och myndigheter.

3.3 Kivra får inte behandla Uppgifterna på något annat sätt, för andra ändamål eller enligt andra instruktioner än de som anges i detta Personuppgiftsbiträdesavtal och Tillämplig Dataskyddslagstiftning. För det fall att Kivra bedömer att det saknas instruktioner som är nödvändiga för att genomföra uppdraget enligt vad som sägs i detta Personuppgiftsbiträdesavtal, eller om Kivra uppmärksammar att instruktionerna strider mot Tillämplig Dataskyddslagstiftning, ska Kivra omedelbart informera Avsändaren om sin inställning samt vidta de åtgärder som Kivra anser är nödvändiga för att uppfylla Tillämplig Dataskyddslagstiftning. Kivra är alltså inte skyldig att följa en instruktion för det fall Kivra anser att instruktionen strider mot Tillämplig Dataskyddslagstiftning.

3.4 Kivra får fortsätta att behandla relevant information från Uppgifterna för egna ändamål i rollen som personuppgiftsansvarig i faktureringssyfte samt i syfte att analysera och förbättra Kivras tjänster till Avsändare. Kivra ansvarar för att informera Användarna om denna behandling i Kivras vid var tid gällande dataskyddsinformation.

4 SÄKERHET – TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER

4.1 Kivra är skyldigt att vidta sådana lämpliga tekniska och organisatoriska åtgärder som uppfyller kraven i Tillämplig Dataskyddslagstiftning, särskilt artikel 32 i Dataskyddsförordningen, och därigenom säkerställa att de Registrerades rättigheter skyddas. Sådana åtgärder innebär bland annat att Kivra skyddar Uppgifterna mot obehörig åtkomst, förstörelse och ändring. En beskrivning av sådana säkerhetsåtgärder finns i Underbilaga B. Kivra förbehåller sig rätten att uppdatera vidtagna säkerhetsåtgärder i Underbilaga B utan att närmare notifiera om detta enligt punkt 10.3.

4.2 Kivra åtar sig att säkerställa att Kivra har sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i Tillämplig Dataskyddslagstiftning, särskilt vad gäller kraven på säkerhet enligt ovan.

5 INFORMATIONSPLIKT OCH ASSISTANS

5.1 Kivra ska utan onödigt dröjsmål efter det att Kivra upptäckt fullbordade fall av eller försök till obehörig åtkomst, förstörelse eller ändring av Uppgifterna och andra personuppgiftsincidenter, informera Avsändaren om detta. För det fall Tjänsten, eller delar av Tjänsten, är otillgänglig av andra anledningar än nyssnämnda händelser, exempelvis vid interna systemstörningar, kommer information om detta att publiceras via kivrastatus.se.

5.2 När Kivra underrättar Avsändaren enligt punkt 5.1 ovan ska underrättelsen innehålla information om:

a) personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet Registrerade som berörs samt de kategorier av och det ungefärliga antalet Uppgifter som berörs,
b) namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
c) de sannolika konsekvenserna av personuppgiftsincidenten, och
d) de åtgärder som Kivra har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

5.3 Om och i den utsträckning det inte är möjligt att tillhandahålla information enligt punkt 5.2 samtidigt, får informationen tillhandahållas i omgångar, dock utan ytterligare onödiga dröjsmål.

5.4 Kivra ska bistå och samarbeta med Avsändaren i en skälig omfattning med att se till att skyldigheterna enligt artiklarna 32–36 Dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som Kivra har att tillgå samt för att säkerställa att Registrerades rättigheter enligt Tillämplig Dataskyddslagstiftning kan uppfyllas.

5.5 Kivra ska utan dröjsmål informera Avsändaren om eventuella kontakter med Tillsynsmyndigheten som rör, eller kan vara av betydelse för, Kivras behandling av Uppgifter. Åtagandet är dock begränsat till sådan behandling av Uppgifter som berör eller kan komma att beröra Avsändaren. Kivra har inte rätt att företräda Avsändaren eller agera för dennes räkning gentemot Tillsynsmyndigheten.

6 GRANSKNING

6.1 Avsändaren har rätt att själv eller genom en oberoende tredje man genomföra kontroller av Kivras behandling av Uppgifterna för att försäkra sig om att vad som anges i Tillämplig Dataskyddslagstiftning, detta Personuppgiftsbiträdesavtalet och de eventuella instruktioner som utfärdats efterlevs. Om annat inte följer av särskild separat skriftlig överenskommelse står respektive Part sina egna kostnader vid granskning och för tillhandahållandet av information enligt denna punkt 6.1.

6.2 Kivra ska i skälig utsträckning bidra till sådana kontroller och granskningar och på begäran tillhandahålla Avsändaren den assistans och den dokumentation som rimligen krävs för detta.

6.3 Om Avsändaren anlitar tredje part att utföra inspektion av Kivras behandling av Uppgifterna för Avsändarens räkning ska Avsändaren tillse att sådan tredje part innan eventuell inspektion undertecknar en ändamålsenlig sekretessförbindelse att inte röja uppgift för tredje man.

6.4 Insyn för granskning, informationslämning och dylikt ska förläggas till tidpunkter på dygnet och i övrigt ske på det sätt som medför minsta möjliga påverkan på Kivras verksamhet. Granskning av Kivra ska ske med iakttagande av de säkerhetsåtgärder som Kivra uppställer förutsatt att åtgärderna inte förhindrar eller medför betydande svårigheter att genomföra granskningen.

7 ANLITANDE AV UNDERBITRÄDEN

7.1 Avsändaren godkänner härmed användandet av de av Kivra redan anlitade underbiträden som framgår av Underbilaga A till detta Personuppgiftsbiträdesavtal.

7.2 Kivra åtar sig att informera Avsändaren om eventuella planer på att anlita av nya underbiträden och/eller ersätta befintliga underbiträden minst trettio (30) dagar innan sådana planer genomförs. Om Avsändaren inte återkommer till Kivra inom de trettio (30) dagarna anses Avsändaren ha accepterat Kivras plan på att anlita/ersätta det/de underbiträde(n) som Kivra informerat Avsändaren om. Om Avsändaren inte godkänner ett underbiträde som Kivra avser att använda åligger det Parterna att samarbeta för att finna en lämplig lösning. Om en lämplig lösning inte kan finnas har Avsändaren rätt att säga upp detta Personuppgiftsbiträdesavtal omgående.

7.3 Kivra åtar sig att teckna ett skriftligt avtal med befintliga och nya underbiträden som reglerar den behandling som underbiträdet utför. I fråga om dataskydd ska avtalet ålägga underbiträdet samma skyldigheter som åläggs Kivra i detta Personuppgiftsbiträdesavtal. För det fall underbiträdet inte uppfyller sina skyldigheter i fråga om behandlingen ska Kivra förbli ansvarig gentemot Avsändaren för underbiträdets uppfyllande av sina skyldigheter enligt detta Personuppgiftsbiträdesavtal.

7.4 Kivra får vidare endast överföra eller på annat sätt behandla Uppgifterna enligt detta Personuppgiftsbiträdesavtal utanför EU/EES om Avsändaren i förväg gett sitt skriftliga samtycke. En överföring till land utanför EU/EES förutsätter även att Kivra, innan överföring påbörjas, uppfyller de krav och åtgärder som följer av Tillämplig Dataskyddslagstiftning, vilket inkluderar att Kivra ska tillse att överföringen sker till länder som av EU-kommissionen beslutats inneha en adekvat skyddsnivå eller vid behov ingå EU-kommissionens vid var tid gällande standardavtalsklausuler.

8 ANSVAR

8.1 Om Part (inklusive den som arbetar under Parts ledning eller av Part anlitat underbiträde) agerar i strid med detta Personuppgiftsbiträdesavtal eller Tillämplig Dataskyddslagstiftning ska sådan Part hålla den andre Parten skadeslös för den eventuella skada som sådant otillåtet agerande orsakat.

8.2 Kivra ska ansvara för skada uppkommen till följd av behandling av Uppgifterna endast om Kivra inte har fullgjort de skyldigheter enligt detta Personuppgiftsbiträdesavtal som specifikt riktar sig till Kivra. Kivra ska undgå ansvar om det visar att Kivra inte på något sätt är ansvarigt för den händelse som orsakade skadan.

8.3 Parts rätt till ersättning enligt punkt 8.1 ska vara begränsad till direkta skador till ett totalt belopp motsvarande fem (5) prisbasbelopp enligt Socialförsäkringsbalken (2010:110) per kalenderår. Under inga omständigheter ska Part vara ansvarig för indirekta skador, såsom utebliven vinst, inkomstförlust, hinder att uppfylla förpliktelse mot tredje man, ersättningsskyldighet mot tredje man eller andra följdskador. Denna ansvarsbegränsning ska dock inte gälla vid grov vårdslöshet eller uppsåt.

8.4 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den Part som påförts en sådan avgift av Tillsynsmyndighet.

8.5 Om endera Part får kännedom om omständighet som kan leda till skada för någon annan Part ska denne omedelbart informera den andra Parten om förhållandet och aktivt arbeta tillsammans för att förhindra och minimera sådan skada.

9 SEKRETESS

Part ska se till att de personer som har åtkomst till Uppgifterna eller konfidentiell information har åtagit sig att iaktta sekretess eller omfattas av lagstadgad tystnadsplikt i enlighet med kraven i Tillämplig Dataskyddslagstiftning samt är informerade om hur de får behandla Uppgifterna.

10 ÄNDRINGAR OCH MEDDELANDEN

10.1 Avsändaren får ändra innehållet i detta Personuppgiftsbiträdesavtal endast i den mån så krävs för att tillgodose krav som följer av Tillämplig Dataskyddslagstiftning. Sådan ändring träder i kraft senast trettio (30) dagar efter att meddelandet om ändring kommit Kivra tillhanda.

10.2 Eventuella justeringar av Avsändarens instruktioner som närmare beskrivs i Underbilaga A ska meddelas av Avsändaren till Kivra i enlighet med punkt 10.4 så att nödvändiga ändringar i rutiner kan genomföras. Kivra har rätt att avsäga sig uppdraget för det fall att Avsändarens instruktioner inte rimligen kan uppfyllas. Sådan ändring träder i kraft senast trettio (30) dagar efter att meddelandet om ändring kommit Kivra tillhanda.

10.3 Kivra förbehåller sig rätten att när som helst ändra och/eller göra tillägg i detta Personuppgiftsbiträdesavtal. Eventuella ändringar och tillägg ska meddelas senast trettio (30) dagar innan ändringen träder i kraft. Kivra har dock alltid rätt att omedelbart vidta sådana ändringar och tillägg som föranleds av Tillämplig Dataskyddslagstiftning eller myndighetsbeslut. Om Avsändaren inte godkänner Kivras ändringar och/eller tillägg, har Avsändaren rätt att säga upp detta Personuppgiftsbiträdesavtal omedelbart.

10.4 Alla meddelanden och annan kommunikation enligt detta Personuppgiftsbiträdesavtal från en Avsändare till Kivra ska ske skriftligen genom e-post till privacy@kivra.com. Alla meddelanden och annan kommunikation från Kivra till Avsändaren ska ske skriftligen genom e-post till den e-postadress som Avsändaren anger. Meddelanden ska anses ha kommit mottagande Part tillhanda samma dag som e-posten mottas. Ansvaret för att hålla sina kontaktuppgifter uppdaterade vilar på respektive Part.

11 AVTALSTID OCH ÅTGÄRDER VID UPPHÖRANDE

11.1 Personuppgiftsbiträdesavtalet gäller från dess undertecknande och så länge som Kivra behandlar Uppgifterna enligt de Allmänna Villkoren.

11.2 Parterna är överens om att Kivra och eventuella underbiträden efter behandlingens upphörande, och beroende på vad Avsändaren instruerar Kivra, utan onödigt dröjsmål men senast inom trettio (30) dagar efter att de Allmänna Villkoren eller Personuppgiftsbiträdesavtalet upphör att gälla ska radera överförda Uppgifter och kopior.

12 TILLÄMPLIG LAG OCH TVISTLÖSNING

Tillämplig lag och tvistlösning följer av de Allmänna Villkoren avsnitt 17.

UNDERBILAGA A: SPECIFIKATION

TJÄNST	ÄNDAMÅL MED BEHANDLINGEN	KATEGORIER AV PERSONUPPGIFTER	KATEGORIER AV REGISTRERADE	TID SOM PERSONUPPGIFTERNA BEHANDLAS FÖR ÄNDAMÅLET	UNDERBITRÄDEN (LOKALISERING)
Betalbara E-försändelser (valbar)	Kivra ska motta och dela uppgifter om betalning med Avsändaren i de fall Avsändaren väljer att få uppgifterna direkt från Kivra och inte via Partner.	Uppgifter om betalning.	Användare.	Maximalt 13 månader.	Ej tillämpligt. (Tink AB, Getswish AB och Trustly Group AB är personuppgiftsansvariga för sina respektive behandlingar av Uppgifterna.)
Swish (valbar)	Kivra ska dela Uppgifter till Getswish AB för att möjliggöra betalning, liksom motta bekräftelse och status på betalningen från Getswish AB.	Uppgifter om betalning.	Användare.	Delningen sker omedelbart.	Ej tillämpligt. (Getswish AB är personuppgiftsansvarig för sin behandling av Uppgifterna.)
Automatisk betalning (valbar)	Kivra ska dela Uppgifter till Trustly Group AB för att sätta upp autogiromedgivanden och möjliggöra betalning, liksom motta bekräftelse och status på autogiromedgivanden och betalning från Trustly Group AB och dela med Avsändaren. Kivra kan även komma att dela Användarens namn för att underlätta Avsändarens felsökning.	Uppgifter om autogiromedgivande och betalning. Uppgifter om namn på Användare.	Användare.	Delningen sker omedelbart. 45 dagar som Hämtningstid för Automatiska betalningar.	Ej tillämpligt. (Trustly Group AB är personuppgiftsansvarig för sin behandlingar av Uppgifterna.)
Campaigns (valbar)	Kivra ska distribuera kampanjer till Användare. För det fall segmentering ska ske, även begränsa listan av Användare som ska exponeras för kampanjen.	Uppgifter som behövs för att distribuera kampanjer. För det fall segmentering ska ske: personnummer.	Användare.	Under den tid som Avsändaren väljer att distribuera kampanjerna eller maximalt 365 dagar. Personnummer raderas omedelbart efter att segmenteringen har skett.	Ej tillämpligt.
Forms (valbar)	Kivra ska tillgängliggöra svar till Avsändaren under Hämtningstiden för Forms i de fall Avsändaren väljer att hämta svaren direkt från Kivra och inte via Partner.	Personuppgifter som förekommer i frågeformuläret. Metadata som tillhör frågeformuläret. Om Avsändaren inhämtar Användares bankkontouppgifter	Användare.	30 dagar.	Om bankkontouppgifter inhämtas: Tink AB som tillhandahåller en tjänst för att verifiera bankkontouppgifter (EU/EES).

		behandlas bankkontouppgifter.			
Rekommenderade E-försändelser (valbar)	Kivra ska tillgängliggöra mottagningsbevis till Avsändaren under Hämtningstiden för Rekommenderade E-försändelser i de fall Avsändaren väljer att hämta mottagningsbevisen direkt från Kivra och inte via Partner.	Personuppgifter som förekommer i mottagningsbeviset, nämligen personnummer, uppgifter om signering med BankID samt metadata från den rekommenderade E-försändelsen.	Användare.	30 dagar.	Ej tillämpligt.

UNDERBILAGA B: SÄKERHET

1 INTRODUCTION

1.1 The goal of this document is to provide transparent, high-level information to Kivra's stakeholders about Kivra's commitment to information security. The document describes Kivra's information security responsibilities and undertakings regarding both the services that Kivra provides to Senders (Sw. *Avsändare*), i.e. the Delivery Service (Sw. *Förmedlingstjänsten*) and any Additional Services (Sw. *Tilläggstjänster*) as well as the services that Kivra provides to Users (Sw. *Användare*). i.e. the digital mailbox (Sw. *digitala brevlådan*). These services are in this document together referred to as the "**Kivra Platform**".

1.2 As Kivra may change its security measures over time, this document may be revised accordingly. Partners and Senders of Kivra can always receive the latest version of this document by contacting Kivra's Security Team as security@kivra.com.

2 KIVRA'S CORPORATE TRUST COMMITMENT

Kivra is committed to achieving and maintaining the trust of our stakeholders. Our goal is to be as transparent as possible with our stakeholders in offering security to meet and exceed expectations in today's ever changing tech landscape.

3 GOVERNANCE

3.1 Policy Ownership

Kivra has a documented Information Security Policy that all employees must read and acknowledge. This policy is approved by the Board of Directors, reviewed and updated annually. Information Security Policy development, maintenance, and issuance is the responsibility of the Kivra CISO.

3.2 Kivra Infrastructure

Kivra hosts the Kivra Platform in a hybrid-cloud environment. Content is hosted in multiple on-premise data centers located within Sweden. The data center facilities are provided by Swedish suppliers, all hardware and software is owned by Kivra and maintained by either our employees or consultants contracted directly by Kivra.

3.3 Third-Party Architecture

Kivra may use one or more third-party suppliers. When doing so, Kivra contractually ensures that these third parties follow adequate security requirements.

Kivra has Risk Management procedures in place that take integrations with, and solutions from, third parties into account on a service/system level. This is governed by the Information Security Policy and the Third Party Risk Management Instruction.

3.4 Audits, Certifications, and Regulatory Compliance

Kivra is connected to the infrastructure Mina meddelanden, governed by the Agency for Digital Governance ("**DIGG**"). As such, Kivra is regularly audited by DIGG towards their ISO27001-based information security requirements.

Kivra's information security is governed by an Information Security Management System (ISMS) that adheres to the ISO 27001 standard.

4 SECURITY CONTROLS

4.1 Organization of Security

Kivra's COO is responsible for the overall Information Security Management of the Kivra Platform, including oversight and accountability. This responsibility is enforced by the Kivra CISO who answers directly to the Kivra COO and leads a Security Team that consists of a Security Subject Matter Expert, Security Engineers and Infrastructure Security. All Business Function/System Owners (Product Owners and Engineering Managers) have Information and IT Security responsibilities within their roles.

The Physical and Personal security of Kivra's offices and employees is the responsibility of the Kivra COO, also coordinated by the Security Team.

4.2 Asset Classification and Logical Access Control

- Kivra maintains an inventory of essential information assets such as servers, databases, and software governed by the IT Policy and the IT Asset Management Instruction.
- Kivra adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff.
- Kivra maintains separate development, sandbox (UAT), staging and production environments. Access to each environment and within each environment is separated and strictly controlled.
- All access to Kivra's servers or data is logged and can only be accessed using multifactor authentication or by users using Mobile Bank-ID.
- Kivra's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.
- Audits on accounts and access are performed regularly.

4.3 Personnel Security and Training

- All employees at Kivra sign a confidentiality agreement when their employment begins. In addition, Kivra conducts background checks for system administrators, developers and other users with privileged access as part of its onboarding process. This also includes key roles within the Kivra Management Team.
- All employees are informed of, and agree to comply with, Kivra's IT- and Information Security policies and practices as a part of their initial on-boarding.
- All Kivra employees undergo security and privacy training as part of their on-boarding and receive frequent training sessions focusing on specific subjects such as phishing.
- Kivra conducts frequent awareness related tests and communicates security related information to all employees and consultants through several internal communication channels.

4.4 Physical and Environmental Security

- Access to Kivra facilities is controlled by 24-hour security. Additionally, all Kivra offices are protected by locked access and are under 24-hour video surveillance (recording triggered by motion). All Kivra employee workstations are encrypted and password protected, and all Kivra user accounts require two-factor authentication.
- Data centers facilities and physical security are provided by Swedish suppliers complying with Kivra contractual requirements.

4.5 Policies and Logging

The Kivra Platform is operated in accordance with the following procedures to enhance security:

- All processing of content is logged monitoring user activity and potential anomalies.
- API key information for third-party services provided by the Sender are encrypted for storage.
- Kivra keeps audit logs for all access to production servers.
- Server access is controlled via public key access, instead of passwords.
- Logs are stored in a secure centralized host to prevent tampering.
- Kivra application and ssh audit logs are stored for five years.
- Passwords are not logged under any circumstances.
- Access to Kivra mail and document services is only allowed on approved workstations and mobile devices that have automated security policies enforced.

4.6 Intrusion Detection

Kivra monitors system, user, and file behavior across its infrastructure using a host-based Intrusion Detection System. Intrusion Detection alerts are monitored by the Security Team and an external SOC.

Kivra's APIs use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and alerts are handled by Kivra's engineering team.

4.7 Security Logs

All Kivra systems used in the provisioning of the Kivra Platform, including firewalls, routers, network switches, and operating systems log information to their respective system log facility or a centralized log server (for network systems) in order to enable security reviews and analysis. Kivra has automated alerts and searches on these logs.

4.8 System Patching and Configuration Management

Kivra patches its servers on a regular basis, which ensures that the latest patches for the software we use are applied. Kivra's configuration management system regularly applies configuration based on repositories.

Kivra maintains multiple environments and tests changes in containerized development environments and in live staging environments before making changes to production environments.

4.9 Vulnerability Management

Kivra's infrastructure and applications are continuously scanned for vulnerabilities. Alerts are monitored by our Security Team. Kivra also maintains a list membership to various CVE vulnerability mailing lists. Patches and vulnerabilities are remediated based on severity. This is governed by the Information Security Policy and the Vulnerability Management Instruction.

In addition, Kivra integrates security into its development process by utilizing static code analysis tools to identify potential vulnerabilities in our codebase before deployment.

4.10 Third-Party Penetration Testing

Kivra undergoes a third-party penetration test of the Kivra Platform on an annual basis. Kivra also conducts our own internal penetration tests in relation to significant changes in our services and environment.

4.11 Monitoring

For technical monitoring, maintenance and support processes, Kivra uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring
- Uptime monitoring
- Functional monitoring
- Database monitoring
- Application Tracing
- Error monitoring
- Office monitoring

4.12 External Access Control

The Kivra Platform employs a variety of security controls. These include, but are not limited to:

- Receiving Users log in to the Kivra Platform using Mobile Bank-ID.
- Senders log in to the Kivra Platform using Google Authentication or OTP.
- All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
- Kivra does not use persistent cookies for sessions.
- Sessions expire after a few hours of inactivity.
- Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.

- Kivra's REST APIs are accessed with separate API keys, which can only be provisioned by Kivra Sender user accounts with administrative access. API keys are granted access to specific API endpoints when created.

4.13 Development and Maintenance

Kivra uses third party tools to effectively manage the development lifecycle. During testing, Kivra generates sandbox accounts and fake data for testing. Kivra does not use production data in sandbox accounts.

Application source control is accomplished through private repositories. Kivra has controls in place to ensure that all code changes are reviewed and implemented by at least two developers before being merged to Kivra's main code branch.

Kivra maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

4.14 Malware Prevention

As a mitigating factor against malware, all Kivra servers run LTS editions of Operation Systems, as well as malware protection functionality.

Kivra provides proper change management to ensure that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All Kivra employee workstations are provided with virus scanners and updated definitions sent out from a central device management platform.

4.15 Information Security Incident Management

Kivra maintains written and regularly tested incident management instructions and procedures. Kivra has 24x7x365 on-call incident management staff. Kivra uses tools to ensure complete coverage with defined escalation policies.

4.16 Data Encryption

The Kivra Platform uses industry-accepted encryption practices to protect Sender data and communications during transmissions between a Sender's network and the Kivra Platform and at rest.

4.17 Return and Deletion of Kivra User Data

The Kivra Platform allows import, export, and deletion of Kivra User data by authorized users at all times during the term of a Kivra User's subscription. Following termination or expiration of the Kivra User subscription, Kivra shall securely overwrite or delete Kivra User data within 20 days following any such termination, in accordance with Kivra's General Terms and Conditions.

4.18 Reliability and Backup

All networking components, SSL accelerators, load balancers, web servers and application servers are configured in a redundant configuration. All Sender data submitted to the Kivra Platform is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

4.19 Business Continuity Management and Disaster Recovery

Kivra has documented Business Continuity procedures. Normal backups are stored in backup servers on-site.

Clusters containing User data use replication to other sites and duplication factors to ensure data redundancy. We also use life-cycle policies to ensure a "delete all scenario" is impossible.

4.20 Mobile Device Management Policies

Kivra uses Mobile Device Management ("**MDM**") platforms to control and secure access to Kivra resources on mobile devices such as phones, tablets, and laptops. Kivra enforces common security settings such as, but not limited to, encryption, lock screen passwords, password expiration, display timeouts, and remote location and remote wipe.

4.21 Blocking Third Party Access

The Kivra Platform has not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access data. We do not provide any government or other third party with encryption keys, or any other way to break our encryption.

5 CONTACTS

Kivra's Security Team can be reached by emailing security@kivra.com.