Global onboarding documents for externals

This document stipulates essential legal obligations! Please read carefully and keep a copy of the document in your files for future consultation.

Table of Contents

1. In General

You or your employer for your benefit (as the case may be) have requested access to the IT systems and/or the premises of Avaloq Group AG and/or its subsidiaries (hereinafter “Avaloq”), as it is required to provide the services and/or deliverables agreed between you or your employer (as the case may be) and Avaloq under a separate project or service agreement (hereinafter “Service Agreement)”. For Avaloq to comply with legal and regulatory requirements and, therefore, as a prerequisite for the granting of such access you are requested to (1.) enter into a personal confidentiality undertaking, (2.) subject to further conditions, assign intellectual property rights to Avaloq, (3.) to commit to adhere to Avaloq’s policies and (4.) acknowledge Avaloq’s information regarding the processing of personal data. By signing the present document on the signature page at the end of the document, you confirm to have read and understood as well as to agree to and being legally bound by the Confidentiality Undertaking, the Assignment of Intellectual Property Rights and the Acknowledgement of Avaloq Policies as contained in this document. Furthermore, you acknowledge the receipt and confirm to understand the content of the Privacy Statement which is also contained in this document.

In particular, but not exclusively, you confirm (subject to the detailed terms and conditions contained in the respective documents):

- In the Confidentiality Undertaking: to keep information and data which is non-public, confidential and/or internal company information and data confidential at all times;
- In the Assignment of Intellectual Property Rights: that all work results, prepared or created by you while providing a service to or working as external staff member for Avaloq (hereinafter “Work Results”), and all rights and entitlements to such Work Results, vest irrevocably to Avaloq and that you transfer and assign to Avaloq any copyrights, utility model rights, design rights, patent rights, trademark rights, trade secret rights, know-how rights as well as any other proprietary or non-proprietary rights pertaining to the Work Results, and assign the property to any copy of Work Results and documentation relating thereto to Avaloq;
- In the Acknowledgement of Avaloq Policies: to know where to retrieve or request Avaloq’s policies, to read them carefully and to adhere to them; and
- In the Privacy Statement: to understand what type of personal data concerning you Avaloq is processing and how it does so.

This document is accepted by all entities of the Avaloq group of companies for the onboarding to their IT systems and/or the granting of access to their premises for a term of three years as of the signature date. All your obligations and all of Avaloq’s rights stipulated in this document will be automatically applicable in relation to all entities of the Avaloq group of companies to whose IT systems and/or premises you are granted access during that three-years term without signing this document again.

2. Confidentiality Undertaking

I, the undersigned, confirm that I am aware of the legal provisions governing the treatment of confidential information (as set out in the relevant Annex to this Confidentiality Undertaking where applicable) and I declare to Avaloq the following:

Confidential Information

I understand that certain information and data which is confidential and/or proprietary information and data (hereinafter "Confidential Information") may/has come to my attention in connection with my visit to Avaloq's premises/the use of Avaloq's IT systems. Confidential Information may have been or might be disclosed to me verbally, electronically and/or in writing by Avaloq, its consultants, its customers and third parties (hereinafter "Disclosing Parties"). In particular, this includes personal data, trade secrets such as the business relationships between Avaloq and its customers and suppliers, any information regarding the clients of Avaloq's customers, Avaloq's technical organisation and equipment (incl. software), the commercial structure of the Avaloq group as well as operational processes. For the avoidance of doubt, it is noted that such information shall be deemed to be Confidential Information, regardless of whether I have obtained knowledge of such information through Avaloq or third parties. Information that is in the public domain shall not be deemed to be Confidential Information, provided that such disclosure is not made by me in violation of this Confidentiality Undertaking or by another person who is not legally authorized to disclose Confidential Information.

Confidential Treatment

I hereby agree

(i) to keep Confidential Information confidential at all times whether or not I (have) become aware of such information before or after signing this document;

(ii) to use the Confidential Information solely for the purpose of my work for Avaloq,

(iii) not to disclose or make accessible Confidential Information to any third party (incl. any other Avaloq subsidiary) except to persons authorized by the Disclosing Party to receive such Confidential Information. However, I am authorized to disclose Confidential Information to my employer as well as to my co-workers on my assignment to Avaloq, but solely on a need to know basis for the services to be provided by me to Avaloq under the Service Agreement;;

(iv) to take all necessary precautionary measures as instructed by my employer or Avaloq or as may expected from a reasonable person working with sensitive information to keep Confidential Information confidential. This includes, in particular, the compliance with all organizational and/or technical security precautions to ensure that unauthorized persons do not have access to and cannot process the Confidential Information contained in the Avaloq documents and files; and

(v) not to take any Confidential Information with me, either as originals or copies, in electronic form (including in photo or print screen form) or as a hard copy, from the electronic systems or premises accessible to me.

I hereby warrant that I am aware of the obligations and restrictions imposed by applicable laws relating to the receipt, handling and the processing of personal data and I undertake that: (i) I will ensure that the integrity of the personal data is maintained; (ii) the personal data will only be used / disclosed for

the stated purpose in which such personal data was obtained; and (iii) the handling and processing of personal data will be carried out in conformance with applicable laws and contractual obligations (data protection).

Disclosure of Confidential Information to the competent authorities shall not constitute a breach of this confidentiality undertaking if and to the extent that such obligation to disclose Confidential Information is required by law, court or governmental order, or as a result of administrative proceedings, provided, however, that I have first notified the Disclosing Party promptly thereof and enabled it to make all reasonable efforts to obtain a protective order or other confidential treatment of the Confidential Information.

Return of Confidential Information upon termination of work

Unless I am instructed otherwise upon termination of my work for Avaloq, I hereby agree to (i) return to Avaloq any Confidential Information in physical form, including any copies I may have made, (ii) transmit any Confidential Information in electronic form to Avaloq, and (iii) confirm in writing (email sufficient) to Avaloq that I have complied with my obligations under (i) and (ii) of this section. I will comply with this obligation without delay and will not retain any copies.

Continuance

I understand and agree that my obligations and Avaloq's rights in accordance with this Confidentiality Undertaking will remain effective for an unlimited period regardless of the completion or termination of my involvement in the service provisioning to Avaloq.

Sanctions

I understand that a breach of this Confidentiality Undertaking may result in serious criminal sanctions (reference is made in particular to the provisions contained in the annexes hereto).

Precedence

In the event of discrepancies between this Confidentiality Undertaking and comparable documents that may have been signed in the past on the same subject, whichever version is the stricter shall prevail.

Annex 1 to the Confidentiality Undertaking: Swiss Legal Provisions

A.) BANK CLIENT CONFIDENTIALITY

Art. 47 Federal Act on Banks and Savings Banks

1 A custodial sentence not exceeding three years or a monetary penalty shall be imposed on any person who wilfully:

a. discloses a secret entrusted to them in their capacity as a director or officer, employee, agent or liquidator of a bank or a person according to article 1b or as a director, officer or employee of an audit company or of which they have become aware in said capacity;

b. attempts to induce a violation of professional secrecy;

c. discloses to other persons a secret disclosed to them in accordance with lit. a or exploits such a secret this information for their own benefit or for the benefit of others.

1bis A custodial sentence not exceeding five years or a monetary penalty shall be imposed on any person who obtains a pecuniary advantage for themselves or another person through an action as detailed in paragraph 1 letter a or c.

2 A fine not exceeding CHF 250,000 shall be imposed on persons who commit the foregoing acts through negligence.

4 Any person who violates professional secrecy remains liable to prosecution after termination of the official or employment relationship or exercise of the profession.

5 The federal and cantonal provisions relating to the duty to testify and the duty to provide information to the authorities are reserved.

6 The cantons are responsible for the prosecution and adjudication of acts described in these provisions. The general provisions of the Swiss Penal Code apply.

B.) SECURITY DEALER'S CONFIDENTIALITY

Art. 69 Federal Act on Financial Institutions; Violation of professional confidentiality

1 A custodial sentence not exceeding three years or a monetary penalty shall be imposed on any person who wilfully:

a. discloses a secret entrusted to them in their capacity as a director or officer, employee, agent or liquidator of a financial institution or of which they have become aware in said capacity;

b. attempts to induce a violation of professional secrecy;

c. discloses to other persons a secret disclosed to them in violation of letter a or exploits such a secret for their own benefit or for the benefit of others.

2 A custodial sentence not exceeding five years or a monetary penalty shall be imposed on any person who obtains a pecuniary advantage for themselves or another person through an action as detailed in paragraph 1 letter a or c.

3 A fine not exceeding CHF 250,000 shall be imposed on persons who commit the foregoing acts through negligence.

4 Any person who violates professional confidentiality remains liable to prosecution after termination of the official or employment relationship or exercise of the profession.

5 The federal and cantonal provisions relating to the duty to testify and the duty to provide information to the authorities are reserved.

6 The cantons are responsible for the prosecution and adjudication of acts under this provision.

C.) PROFESSIONAL SECRECY

Art. 162 Swiss Penal Code; Breach of manufacturing or trade secrecy

Any person who betrays a manufacturing or trade secret that he is under a statutory or contractual duty contract not to reveal,

any person who exploits for himself or another such a betrayal,

is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.

D.) INSIDER TRADING

Art. 154 Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading; Exploitation of insider information

1 A custodial sentence not exceeding three years or a monetary penalty shall be imposed on any person who as a body or a member of a managing or supervisory body of an issuer or of a company controlling or controlled by them, or as a person who due to their holding or activity has legitimate access to insider information, if they gain a pecuniary advantage for themselves or for another with insider information by:

a. exploiting it to acquire or dispose of securities admitted to trading on a trading venue in Switzerland or to use derivatives relating to such securities;

b. disclosing it to another;

c. exploiting it to recommend to another to acquire or dispose of securities admitted to trading on a trading venue in Switzerland or to use derivatives relating to such securities.

2 Any person who through an act set out in paragraph 1 gains a pecuniary advantage exceeding one million francs shall be liable to a custodial sentence not exceeding five years or a monetary penalty.

3 Any person who gains a pecuniary advantage for themselves or for another by exploiting insider information or a recommendation based on insider information disclosed or given to them by a person referred to in paragraph 1 or acquired through a felony or misdemeanour in order to acquire or dispose of securities admitted to trading on a trading venue in Switzerland or to use derivatives relating to such securities shall be liable to a custodial sentence not exceeding one year or a monetary penalty.

4 Any person who is not a person referred to in paragraphs 1 to 3 and yet who gains a pecuniary advantage for themselves or for another by exploiting insider information or a recommendation based on insider information in order to acquire or dispose of securities admitted to trading on a trading venue in Switzerland or to use derivatives relating to securities shall be liable to a fine.

E.) PROHIBITION OF INDUSTRIAL ESPIONAGE

Art. 273 Swiss Penal Code; Industrial espionage

Any person who obtains a manufacturing or trade secret in order to make it available to an external official agency, a foreign organisation, a private enterprise, or the agents of any of these, or,

any person who makes a manufacturing or trade secret available to an external official agency, a foreign organisation, a private enterprise, or the agents of any of these,

is liable to a custodial sentence not exceeding three years or to a monetary penalty, or in serious cases to a custodial sentence of not less than one year. Any custodial sentence may be combined with a monetary penalty.

F.) DATA PROTECTION

Art. 35 Federal Act on Data Protection; Breach of professional confidentiality

1 Anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their professional activities where such activities require the knowledge of such data is, on complaint, liable to a fine.

2 The same penalties apply to anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their activities for a person bound by professional confidentiality or in the course of training with such a person.

3 The unauthorised disclosure of confidential, sensitive personal data or personality profiles remains an offence after termination of such professional activities or training.

Annex 2 to the Confidentiality Undertaking: German Legal Provisions

This selection of legal provisions is intended to give you an overview of the relevant confidentialty legislation. It is provided by way of example and is by no means exhaustive. Further information is available from your legal department.

Section 4 German Act on the Protection of Trade Secrets (GeschGehG) - Prohibited actions

(1) A trade secret must not be obtained by means of

1. unauthorized access to, appropriation or copying of documents, objects, materials, substances or electronic files that are under the lawful control of the owner of a trade secret and that contain the trade secret or from which the trade secret may be derived, or

2. any other conduct which, in the particular circumstances, does not comply with the principle of good faith, having regard to honest market practices.

(2) A trade secret must not be used or disclosed by anyone who

1. has obtained the trade secret by means of their own actions under paragraph 1
   (a) point 1, or
   (b) point 2

2. violates an obligation to limit the use of the trade secret, or

3. violates an obligation not to disclose the trade secret.

(3) A trade secret must not be obtained, used or disclosed by anyone who has obtained the trade secret through another person and who, at the time of obtaining, using or disclosing it, knows or ought to know that the other person has used or disclosed the trade secret contrary to paragraph 2. This applies in particular if the use consists of producing, offering, placing on the market or importing, exporting or storing illegal products for these purposes.

Section 201 German Criminal Code (StGB) - Violation of privacy of spoken word

(1) A penalty of imprisonment for a term not exceeding three years or a fine shall be imposed on any person who without authorization

1. makes an audio recording of the privately spoken words of another or

2. uses or makes a recording thus produced available to a third party.

(2) The same penalty will be imposed on whoever, without being authorized to do so,

1. uses a listening device to intercept the privately spoken words of another which they are not intended to hear, or

2. publicly communicates, verbatim or the essential content of, the privately spoken words of another which were recorded as per subsection (1) no. 1 or intercepted as per subsection (2) no. 1.

The act referred to in sentence 1 no. 2 only entails criminal liability if the public communication is suitable for interfering with the legitimate interests of another. It is not unlawful if the public communication was made for the purpose of safeguarding overriding public interests.

(3) Whoever, in the capacity as a public official or a person entrusted with special public service functions, violates the privacy of the spoken word (subsections (1) and (2)) incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(4) The attempt is punishable.

(5) The audio recording and listening devices which the offender or participant used may be confiscated. Section 74a applies.

Section 202a StGB - Data espionage

(1) Whoever, without being authorized to do so, obtains access, by circumventing the access protection, for themselves or another, to data which were not intended for them and were specially protected against unauthorized access incurs a penalty of imprisonment for a term not exceeding three years or a fine.

(2) For the purposes of subsection (1), data are only those which are stored or transmitted electronically, magnetically or otherwise in a manner which is not immediately perceptible.

Section 202b StGB - Phishing

Whoever, without being authorized to do so, intercepts data (section 202a (2)) which are not intended for them, either for themselves or another, by technical means from non-public data transmission or from an electromagnetic broadcast from a data processing facility incurs a penalty of imprisonment for a term not exceeding two years or a fine, unless the offence is subject to a more severe penalty under other provisions.

Section 202c StGB - Acts preparatory to data espionage and phishing

(1) Whoever prepares the commission of an offence under section 202a or 202b by producing, acquiring for themselves or another, selling, supplying to another, disseminating or making available in another way

1. passwords or other security codes which provide access to data (section 202a (2)) or
2. computer programs for the purpose of the commission of such an offence

incurs a penalty of imprisonment for a term not exceeding two years or a fine.

(2) Section 149 (2) and (3) applies accordingly.

Section 303a, para. 1 StGB:

Whoever unlawfully deletes, suppresses, renders unusable or alters data [...] incurs a penalty of imprisonment for a term not exceeding two years or a fine.

Section 823 German Civil Code (BGB) - Liability in damages

(1) A person who, intentionally or negligently, unlawfully injures the life, body, health, freedom, property or another right of another person is liable to make compensation to the other party for the damage arising from this.

(2) The same duty is held by a person who commits a breach of a statute that is intended to protect another person. If, according to the contents of the statute, it may also be breached without fault, then liability to compensation only exists in the case of fault.

Secrecy of telecommunications

Act on Data Protection and Privacy in Telecommunications and Telemedia (Telecommunications-Telemedia Data Protection Act- TTDSG) Section 27 Penalty provisions

(1) A penalty of imprisonment not exceeding two years or a monetary penalty shall be imposed on anyone who

1. Listens to a message or takes note of it in a comparable manner in contravention of Section 5 (1),

2. makes a communication in contravention of Section 5 (2), first sentence, or

3. in contravention of Section 8 (1), manufactures or makes available on the market a telecommunications system referred to therein.

(2) If the offender acts negligently in the cases referred to in subsection (1) number 3, the penalty shall be imprisonment for up to one year or a fine.

Protection of personal data under the German Social Code (SGB)

Section 78 para. 1 second and third sentences SGB Book X

The transmission of social data pursuant to Sections 68 to 77 or pursuant to another legal provision in this Code to a non-public body at the latter's request shall only be permissible if the latter has given an undertaking to the transmitting body that it will process the data only for the purpose for which they are transmitted to it. The third parties shall keep the data secret to the same extent as the bodies referred to in Section 35 of the First Book of the Code.

Annex 3 to the Confidentiality Undertaking: UK Legal Provisions

A.) BANK CLIENT CONFIDENTIALITY

Bank clients right to confidentiality in the UK

Banking customers in the UK enjoy protection afforded by the terms of the banking relationship between the customers and the bank. By extension Avaloq is responsible to its clients to ensure the maintenance of confidentiality of bank customer information.

This obligation is assumed by each supplier personnel who is provided with access to Avaloq's IT systems and/or premises.

B.) INSIDER TRADING AND MARKET ABUSE

Insider Dealing and Unlawful Disclosure

It is a criminal offence under the Criminal Justice Act for any person to deal in or encourage another person to deal in any securities about which they have insider information, or pass on any such information other than in the course of the performance with their responsibilities

It is an offence to deal in or attempt to deal in financial instruments including cancelling or amending and existing order, on which such person has inside information, or to recommend or induce another person to transact on the basis of inside information.

Market Abuse

Disclosure of inside Information otherwise than in the proper course of the exercise of the employment, profession or duties is forbidden.

3. Assignment of Intellectual Property Rights (in particular Copyrights) to Avaloq

The transfer and assignment of rights, claims, interests and entitlements to Avaloq as set out in the present document shall not apply if and to the extent that:

EITHER

- I am under any materially equivalent statutory or contractual obligation to transfer and assign such rights, claims, interests and entitlements to my employer; and (cumulatively)
- my employer has agreed in the Service Agreement to transfer and assign these rights, claims, interests and entitlements to Avaloq, independent under which terms and conditions or if similar or equal to the terms of this present document.

OR

- Avaloq and my employer have agreed in the Service Agreement that such shall remain with my employer.

If the before mentioned conditions are not applicable, the following shall apply:

I acknowledge and agree that all work results, including all intermediate and/or partial versions thereof, prepared or created by the Undersigned (hereinafter "Work Results") while providing a service to or working as external staff member for any Avaloq group company, and all rights and entitlements thereto, vest irrevocably to the respective entity of the Avaloq group of companies (hereinafter "Avaloq") and that Avaloq will be the sole and exclusive owner of such Work Results and all rights and entitlements thereto, and of the copies and documentation relating thereto.

Work Results include, but are not limited to, concepts, ideas, methods, methodologies, studies, software, user interfaces, screen designs, HTML codes, flow charts, diagrams, notes, outlines, lists, texts, compilations, manuscripts, writings, pictorial materials, schematics, designs, specifications, inventions, improvements, ideas, techniques, procedures, processes, know-how, and other creations, material, information and the like, whether or not protected by law.

I hereby transfer and assign to Avaloq any copyrights, utility model rights, design rights, patent rights, trademark rights, trade secret rights, know-how rights as well as any other proprietary or non-proprietary rights pertaining to the Work Results, including any claims, interests and entitlements to apply for the registration of such rights, and assigns the property to any copy of Work Results and documentation relating thereto to Avaloq. This transfer and assignment encompass any and all rights, claims, interests and entitlements pertaining to Work Results and is unlimited. It includes, but is not limited to, any rights to make, to use, to perform, to exploit and distribute and to modify the Work Results, and to prepare derivative works and compilations thereof.

This transfer and assignment are worldwide. To the extent as the laws of a particular jurisdiction do not provide for the possibility to transfer and assign such rights, I grant Avaloq an exclusive, perpetual, assignable, irrevocable, unrestricted and unlimited license to make, to use, to perform, to exploit and distribute, to sublicense and to modify the Work Results, and to prepare derivative works and compilations thereof.

I herby waive my rights, if any, to be named as author or inventor of Work Results. I waive, as against

Avaloq (including its affiliates, assignees and licensees), all moral rights which I have acquired or acquire during my engagement for Avaloq and agree to enforce moral rights as against others, as directed by and at the cost of Avaloq (or its affiliates).

I shall promptly and fully disclose and deliver the Work Results to Avaloq, and shall execute and deliver any and all applications, assignments, confirmations and other documents that Avaloq may require in order to protect or defend the Work Results.

4. Acknowledgement of Avaloq's Policies

I declare to Avaloq to have received, read and understood the attached policies and that I will adhere to them (as amended from time to time).

As soon as access to Avaloq's IT systems is granted, I will consult the additional policies, directives and regulations (global and local ones) applicable to me – which are available on the Intranet or upon request from my Avaloq line manager or Avaloq's contact person – and I will inform my Avaloq line manager / Avaloq contact person immediately in case I am not able or willing to fully comply with these additional documents. In case of uncertainties, I will consult my Avaloq line manager or Avaloq's contact person.

Attachments:

- Global Policy Information Security;
- Global Policy Acceptable Use (special attention is drawn to the provisions regarding logging);
- Global Policy Anti-Bribery and Anti-Corruption;
- Global Policy Data Protection;
- Global Policy External Communications; and
- Global Policy Conflict of Interests
- Global Policy Whistleblowing.

5. Privacy Statement

About this Statement

This Privacy Statement (hereinafter “Statement”) explains how Avaloq processes Consultant personal data in the context of a contractual relationship between the Consultant or his/her employer and Avaloq.

Avaloq is committed to providing transparent information about its data processing activities and to keeping Consultant personal data safe. This applies to all Avaloq affiliates worldwide and is based on globally accepted data protection requirements.

The subjects addressed by this Statement are: current and former consultants, supplier personnel, independent contractors and agents (herein collectively referred to as “Consultants”).

Processing of Personal data

Avaloq collects personal data directly from the Consultants. However, it is possible that personal data is collected from a third party, or that personal data is generated by Avaloq itself.

Avaloq may process:

- Personal information and contact details: Including but not limited to full name, birth name, address, telephone number, e-mail address, age, date of birth, gender, marital status, information about relatives, emergency contact information, pictures, place of birth, nationality, children’s names and dates of birth, government-issued identity documents, social security number, information regarding criminal records, information regarding debt prosecution and sanction lists, work permits and residence permits;
- Information in connection with the performance of the Service Agreement: Including but not limited to job description, data on joining and resigning from the company, salary, position, line managers, initials, correspondence with the Consultants, dates of business trips (e.g. plane and train tickets, hotel reservations, etc.), working hours, business contacts, military status, memberships and representation in associations and other organizations and committees, vacation and sick leaves, other absences, information regarding possible health, religious and other requirements, trade union-related information as far as required, login, directory and account data of the systems of Avaloq and further information in connection with various applications, information regarding access controls and their logs, camera recordings on the premises and in production, specific professional or personal skills, and preferences or opinions as disclosed by the Consultants in internal interviews or discussions, questionnaires or dedicated survey tools or internal social networks;
- Education, training and qualifications: Including but not limited to education and degrees, references and interim job reports, curriculum vitae, and qualifications;
- Business records containing information that may refer to the Consultants in an identifiable manner: Including but not limited to e-mails, minutes, reports, forms, memorandums, notes to file, contracts, presentations, further documents, and audit trails in systems.

Wherever possible and prior to the collection of personal data, Avaloq will indicate if it is mandatory for the Consultants to provide certain personal data and the consequences of not providing it.

Processing of sensitive personal data

Sensitive personal data is subject to enhanced protection. Avaloq will only process sensitive personal data where this is strictly necessary and allowed or required by law or if the Consultants have given their consent to process it. Avaloq will always consult with the data protection officer prior to processing sensitive personal data for a given purpose.

Sensitive personal data includes data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health-related data, genetic data, biometric data or data concerning a person's sex life or sexual orientation.

Purpose of personal data processing and lawful basis

Avaloq may only process personal data with a valid legal basis. Avaloq's legal basis and processing purposes are listed below (list not exhaustive):

A) Contractual/pre-contractual obligations:

- Examination of Consultants' suitability, including verification of qualifications, conducting a background check and periodic repetition of such verification and checks regarding positions, where this is necessary;
- Service Agreement and related duties, e.g. insurance processing, notifications to authorities, recording of working hours, identification and authentication in connection with access control;
- Transfer between different Avaloq entities;
- Relocation of Consultants;
- Performance of other service-related contracts with the Consultants;
- Various processes in connection with the administration of the Consultants' data, e.g. organization of business trips, participation in events and associations, organizations and other committees, invoices of services rendered by third parties which the Consultants have used.

B) Legitimate interests:

- Use of work products;
- Ensuring business operations, e.g. operation of IT systems, support hotlines;
- Mergers and acquisitions and other corporate transactions;
- Content for the internet, intranet and other publications, e.g. Consultant directory, customer magazines, advertisement and public relations;
- Organization and realization of company events, photographic documentation of such events;
- Representation, e.g. at customer events, job fairs and in social networks;
- Activities in connection with special events, e.g. birthdays, child births, anniversaries;
- Statistics, e.g. statistics regarding staff, non-personalized statistics regarding work performance, statistics regarding the use of resources of Avaloq (systems, intranet, premises).

C) Compliance with legal obligations:

- Security and safety reasons e.g. workplace safety, safety and security of premises including entrance controls, system security, protection of data, and the secrets and assets of or entrusted to Avaloq;
- Investigations, legal proceedings, compliance, e.g. investigations of possible misconduct of Consultants, necessary internal surveillance and investigation measures in accordance with legal and other provisions and internal regulations, participation in official investigations and proceedings, and establishment and exercise of and defence against legal claims.

Changes to the processing purpose and lawful basis are only possible to a limited extent and require a case-by-case substantiation by the data protection officer.

Protection and security of personal data

Avaloq takes the protection of the Consultants' personal data very seriously. It is subject to strict confidentiality and data secrecy. Avaloq takes appropriate security measures – including administrative, technical and physical measures – to maintain and protect the Consultants' personal data against loss, theft, misuse, unauthorized access, disclosure, alteration and destruction. Access to the Consultants' personal data is restricted to authorized personnel only and kept to a minimum to protect their privacy. This applies regardless of whether data is processed electronically or in paper form.

Retention of personal data

As a rule, Avaloq retains Consultant personal data for the duration of the ongoing service provisioning and for ten years after termination of the services. For more sensitive Personal Data, i.e. criminal record extract, debt register extract, copy of passport/ID, where applicable a retention period of a maximum of three years after offbarding the Consultant applies. Longer statutory retention might be permissible if valid reason exists.

Transfer of personal data

Avaloq transfers personal data within Avaloq affiliates as well as to third parties, for example service providers. Avaloq will only transfer data when measures are in place to guarantee adequate protection. Avaloq's internal personal data transfers are based on Avaloq's Intra-Group Data Transfer Agreement signed by all Avaloq affiliates. The Intra-Group Data Transfer Agreement is available upon request.

Any personal data transfer is based on a strict need-to-know basis and for the recipient to execute a specific purpose. Any personal data transfer undertaken without a strict need-to-know basis, by Consultants or others, would breach applicable privacy laws and Avaloq's data protection policies.

Categories of third parties that could receive some of the Consultants' personal data are: service providers, including dealers, suppliers and other business partners; clients of Avaloq; local, national and foreign authorities; the media; the public, including visitors of websites and social media of Avaloq; associations, organizations, other committees and industry organizations; competitors; future employers, landlords and other third parties to whom Avaloq may provide references about the Consultants; acquirers and prospective acquirers of business divisions, companies or other parts of Avaloq; other parties in potential or actual legal proceedings; and further companies of Avaloq (collectively referred to as "third parties").

Consultants' rights and responsibilities

The Consultants must inform Avaloq immediately if their personal data changes over the course of their working relationship with Avaloq.

The Consultants may request information from Avaloq regarding the processing of their personal data. The Consultants have the right to request the correction, destruction or restriction of their personal data as well as to object to its processing. Requests in this respect must be submitted to dataprotection@avaloq.com. Avaloq reserves the right to restrict the Consultants' rights to those granted by applicable privacy laws.

Should the processing of personal data be based on consent, the Consultants may withdraw their consent at any time. Such withdrawal will not have retroactive effect. Avaloq reserves the right to base the processing of personal data on one or more different legal bases.

If the Consultants believe that the processing of their personal data violates applicable privacy law requirements, the Consultants have the right to lodge a complaint with a competent supervisory data protection authority. Competent authorities can be identified based on the list below:

Australia: OAIC	France: CNIL	Germany: BfDI
Hong Kong: PCPD	Luxembourg: CNPD	Singapore: PDPC
Spain: AEPD	Switzerland: FDPIC	The Philippines: NPC
United Kingdom: ICO		

Amendments

Avaloq will amend this Statement whenever changes are necessary and will communicate such changes in an appropriate manner.

Contact details

If the Consultants have any questions or comments with respect to the processing of their personal data or wish to exercise their rights under applicable privacy laws, please contact dataprotection@avaloq.com. Alternatively, the Consultants can refer to their local data protection officer:

Switzerland
Maria Münch
Maria.Muench@avaloq.com
+41 58 316 25 31

EMEA
Daniel Selig
Daniel.Selig@avaloq.com
+49 30 915 808 264

APAC
Stephen Koh
Stephen.Koh@avaloq.com
+65 6347 56 16

The Philippines
Xander Ganado
XanderPreslie.Ganado@avaloq.com
+41 58 316 34 72

6. Applicable Law and Competent Jurisdiction

Applicable Law

With regard to my legal relationship with any particular entity of the Avaloq group of companies to whose IT systems and/or premises I'm granted access to, the provisions of this document are in all respects governed by and construed in accordance with the same substantive law as the place where the Avaloq entitiy, to which I am onboarded, has its registered office.

Competent Jurisdiction

Any disputes arising out of or in connection with this document are subject to the exclusive jurisdiction of the same courts where the onboarding Avaloq entity has its registered office. Notwithstanding the foregoing, Avaloq remains entitled to seek injunctive relief wherever any infringement of this document occurs or appears imminent.

7. Signature

I hereby confirm that I have read and understood the rights and obligations specified herein (in particular in the Confidentiality Undertaking, the Assignment of Intellectual Property Rights, the Acknowledgement of Avaloq Policies and the Privacy Statement) as well as the provisions regarding the place of jurisdiction and the applicable law. I undertake to abide by the aforesaid terms.

Place, date	Name of employer/supplier
Punganur, 22-04-2024	HCL TECH
Name, surname (in block letters)	Signature
Rajani Dodamaladoddi	