AGILENT TECHNOLOGIES - GDPR PRIVACY POLICY

Agilent Technologies reserves the right to amend, suspend or withdraw any part of this policy at its absolute discretion. It does not form part of your contract of employment.

Updated August 10, 2022

1.1 Purpose

This GDPR Privacy Policy (the "**Policy**") details the personal data your employer ("**Company**", "**Agilent**", "**we**", "**us**" or "**our**") receives about you, how your employer process it and your rights and obligations in relation to your personal data during the course of your employment. Your employer is the data controller for the purposes of the General Data Protection Regulation, any other European Union Law or any relevant local legislation ("**Data Protection Laws**"). In the first instance, should you need to discuss this policy please contact Agilent's Data Protection Officer whose details are set out at clause 1.2 of this Policy.

Location	**Employer**	**Contact details**
Austria	Agilent Technologies Osterreich GmbH	Mooslackengasse 17 1190 Wien
Belgium	Agilent Technologies Belgium N.V./S.A.	Pegasus Park, De Kleetlaan 5 Bus 9 1831 Diegem
Denmark	Agilent Technologies Denmark ApS	Produktionsvej 42 DK-2600 Glostrup
Finland	Agilent Technologies Finland Oy	Hevosenkenkä 3 02600 Espoo
France	Agilent Technologies France SAS	Parc Technopolis / Z.A. Courtaboeuf 3, Avenue du Canada CS 90263 91978 LES ULIS Cedex
Germany	Agilent Technologies Sales & Services GmbH & Co. KG	Hewlett-Packard-Str. 8 76337 Waldbronn Germany
Germany	Agilent Technologies Manufacturing GmbH & Co. KG	Hewlett-Packard-Str. 8 76337 Waldbronn Germany

Germany	Agilent Technologies R&D and Marketing GmbH & Co. KG	Hewlett-Packard-Str. 8 76337 Waldbronn Germany
Germany	Agilent Technologies Deutschland GmbH	Hewlett-Packard-Str. 8 76337 Waldbronn Germany
Ireland	Agilent Technologies Ireland Limited	Unit 3, Euro Business House Little Island Co. Cork Ireland
Italy	Agilent Technologies Italia S.p.A	Via P. Gobetti 2/C 20063 Cernusco sul Naviglio MI
Netherlands	Agilent Technologies Netherlands B.V.	Laan van Langerhuize 1, toren A-8 1186 DS Amstelveen
Norway	Agilent DGG Norway AS	Postboks 4814 Nydalen N-0422 Oslo
Spain	Agilent Technologies Spain, S.L.	Parque Empresarial Alvia Calle Jose Echegaray, 8 - Edificio 3 - Planta 1 28232 Las Rozas, Madrid (Spain)
Sweden	Agilent Technologies Sweden AB	Kronborgsgrand 1 Floor 3 164 46 Kista
United Kingdom	Agilent Technologies LDA UK Limited	Lakeside 5500 Cheadle Royal Business Park Stockport, Cheshire SK8 3GR

1.2 Data Controller Contact Details

For all data privacy inquiries and any questions or concerns you have about this Policy, please contact the Chief Privacy Officer, whose name and contact details are listed below:

Name: Leslie Stevens

E-mail: leslie.stevens@agilent.com
Phone: +1 408 553 4323
Post: 5301 Stevens Creek Blvd. Santa Clara, CA 95051

In addition, as required under applicable law, you may also contact Agilent's Data Protection Officer under GDPR:

Name: Malene Fagerberg, Partner Cyber Security, Deloitte Denmark
E-mail: data-protection.officer@agilent.com
Phone: +45 36 10 20 30
Post: Deloitte Statsautoriseret Revisionspartnerselskab
Weidekampsgade 6, 2300 København S, Danmark

1.3 Scope

"**Data subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

"**Employee(s)**" means employees engaged under a contract of employment and shall also, for the purposes of this Statement, and not, for the avoidance of doubt, for any other reason including co-employment, include any individuals engaged by Agilent on a Non-Agilent Worker contract basis.

"**Personal data**" means any information relating to a Data Subject.

"**Non-Agilent Worker**" means any person who is working or providing services for Agilent and is not an Employee, including external temporary workers and independent contractors.

"**Sensitive personal data**" is Personal Data that reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for the purpose of uniquely identifying you), physical or mental health, or sex life or sexual orientation.

Data Protection Laws prescribe the way in which Agilent may collect, retain and handle personal data (including sensitive personal data). Agilent will comply with the requirements of the Data Protection Laws, and all employees and contractors who handle personal data in the course of their work must also comply with it (see further Section 1.8 (*Your Obligations in Relation to Personal Data)* below).

Data Protection Laws require that any personal data held by Agilent should be processed according to the principles set out below. Personal data should:

(a) be processed fairly and lawfully, and in a transparent manner;

(b) be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes;

(c) be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) not be kept in a form which permits identification of a living individual for longer than is necessary for the purposes for which the personal data is processed; and

(f) be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Laws also provide employees with certain rights, as outlined at Section 1.7 (*Your Rights in Relation to Your Personal Data Held by Agilent*) below.

Applicable works council agreements may also specify the principles and data subject rights further and we would ask you to review those Agilent works council agreements that apply in your country.

1.4 What information does Agilent Collect about Employees and Non-Agilent Workers?

Agilent holds personal data about you. If this information changes, please let us know at the earliest opportunity so that our records can be updated (see Section 1.8 (*Your Obligations in Relation to Personal Data*) below for more details).

Where permitted or required by local law, Agilent will collect the following personal data about you as part of your relationship with Agilent as an Employee or a Non-Agilent Worker:

(a) identity information such as title, full name, gender, citizenship, nationality date of birth, photograph, passport or other unique ID number, driver's license copies or driver's license numbers, and proof of eligibility to work and details of any work permit application;

(b) contact details such as home and work address, phone number(s), email address(es), emergency contacts and next of kin;

(c) personal and family details such as place of birth, name of partner/spouse, number of children, date of birth of partner/spouse, occupation/education details of partner/spouse/children/dependents, marital status, dependent information, language, family composition, religious beliefs, political beliefs and trade union membership where allowed by law;

(d) health information including physical and mental health or condition, disabilities, sickness absence records, accident reporting, occupational health information, meal preferences, and food allergies, and health number;

(e) data with respect to career management and development, including date of hire, employee category, full/part-time status, qualifications, references, resumé(s) or curriculum vitae, language(s) spoken, background checks (including criminal records);

(f) compensation, benefits and other financial data, including current and past salary details, records of your benefits entitlements and utilisation, your bank or building society account details, tax/social security number, bonuses, expenses, pensions, and vehicle details (of company car), payments to family and dependents;

(g) data with respect to the execution of the employment contract or engagement, including presence and absence, work schedules, responsible duties, employee ID, time recording, vacation, maternity/paternity leave, secondments, training records, notes regarding discussions between yourself and Agilent management, performance appraisals and documents relating to corrective action for performance issues, retirement and termination of employment or engagement and related data including notice periods;

(h) data related to use of building access control systems, including time and location of entry and exit, access to restricted zones and security camera footage data related to access to and usage of office equipment and resources including but not limited to fixed and mobile phones, computer systems, email and the internet, cost recovery systems, document management systems, contact management systems and online databases; and

(i) data related to travel for the purposes of the working relationship or as part of employee benefits programmes, relocation, or job reorganisation.

Agilent will monitor use of your work email account, phone lines (including any mobile provided by the Agilent for your business use) and the internet while on company systems in accordance with applicable local laws and Agilent's Acceptable Use policy found here.

We receive information about you directly from you, as well as from other sources including Agilent systems, benefits providers, third parties such as past employers, and our Recruitment partners.

1.5 How does Agilent use your Personal Data?

Agilent will use your personal data for the purposes set out in the table in Appendix 1. This table also sets out the legal basis for processing relied upon by Agilent to process your personal data.

Your personal data will be processed in accordance with the data processing principles set out in Section 1.3 (*Scope*) of this Policy.

Personal data relating to your family members or friends will be processed by Agilent for a variety of reasons, such as the administration of pension and/or retirement plans, health insurance programs and schemes, employment termination, mandatory reporting requirements, the payroll and leave management, and as a contact in emergency situations. It is your responsibility to inform your family and friends members about the processing of their personal data for the described purposes and to confirm that they have given their permission.

Your personal data will be retained by Agilent in accordance with the time periods and in the format specified in the General Retention Schedule.

In the following circumstances, your personal data may be retained for longer than the specified periods:

(a) as required by law or court order;

(b) as needed to defend or pursue legal or regulatory claims; and

(c) in line with specify any relevant industry codes of practice

1.6 Disclosure of your Personal Data and Transfers Overseas

Disclosures and transfers within Agilent

Agilent takes all necessary security and legal precautions to ensure the safety and integrity of personal data that is transferred within its group. Where a transfer of personal data within Agilent involves a transfer of personal data outside the European Economic Area ("**EEA**"), we rely on Standard Contractual Clauses (see below).

The personal data that we collect from you will be transferred to, and stored at/processed in the United States, under the Commission's model contracts for the transfer of personal data to third countries (i.e., the standard contractual clauses), pursuant to Decisions 2004/915/EC and 2010/87/EU. Please contact the Data Protection Officer should you wish to examine the intra-group standard data protection clauses entered into by Agilent.

Disclosures and transfers to third parties

Your personal data will, in certain circumstances, be disclosed to third parties for the purposes described in Appendix 1. These third parties include:

(i) Payroll and benefit providers;

(ii) Financial institutions, pension providers and insurance providers;

(iii) Occupational Health providers and other medical providers/agencies;

(iv) Learning Providers;

(v) Application Support providers, cloud providers, and IT service providers;

(vi) Travel Service providers;

(vii) Time Management and Recruitment providers; and

(viii) Legal counsel and accountants.

Where Agilent is under an obligation to do so by law, it will disclose your personal data to regulators, courts, the police or tax/government authorities, or in the course of litigation, in response to an emergency which threatens persons or property, when necessary to protect the legal interests of Agilent, and when required for reasons of national security/ prevention or detection of crime. In some cases, in accordance with applicable law, it may not be possible to notify you in advance about the details of such disclosures. Agilent will use all reasonable efforts to disclose the minimum personal data necessary in such cases. All such requests shall be referred to HR and/or Legal Compliance who may, at their sole discretion, request proof of entitlement and/or exemption under the Data Protection Laws and proof of identity, before releasing any information.

Personal data may also be disclosed to a third party such as a bank, mortgage company, lender, credit agency, landlord, prospective employer, relocation company, visa or travel agency, but only at your request and with your consent.

Agilent uses a number of third party suppliers (as noted above) to provide services to Agilent. All suppliers that process personal data outside of the EEA are required to execute the Standard Contractual Clauses for the transfer of personal data or otherwise have a legal basis for transferring personal data to Third Countries in compliance with GDPR.

1.7 Your rights in relation your Personal Data held by Agilent

You have certain rights in relation to the personal data we hold about you. Some of these only apply in certain circumstances as set out in more detail below. We also set out how to exercise those rights. Please note that we will require you to verify your identity before responding to any requests to exercise your rights by providing: in the case of an Employee, (i) a valid employee email address; and (ii) a valid employee ID number, or in the case of a Non-Agilent Worker, name and valid proof of ID (e.g. driver's license or passport). We must respond to a request by you to exercise those rights without undue delay and at least within one (1) month (although this may be extended by a further two (2) months in certain circumstances). To exercise any of your rights, please fill out the following form here or address your request to data-protection.officer@agilent.com

(a) You have the following rights in relation to your personal data:

(i) *Access*: to access the personal data held by Agilent about you and certain information about how we use it and who we share it with.

(ii) *Portability*: in certain circumstances, you have the right to receive or ask us to provide your personal data to a third party in a structured, commonly used and machine-readable format, although we will not provide you with certain personal data if to so would interfere with another's individual's rights (e.g. where providing the personal data we hold about you would reveal information about another person) or where another exemption applies (we can only do so where it is technically feasible; we are not responsible for the security of the personal data or its processing once received by the third party).

(iii) *Correction*: to correct any personal data held about you that is inaccurate and have incomplete data completed (including by the provision of a supplementary statement). Where you request correction, please explain in detail why you believe the personal data we hold about you to be inaccurate or incomplete so that we can assess whether a correction is required. Please note that while we assess whether the personal data we hold about you is inaccurate or incomplete, you may exercise your right to restrict our processing of the applicable data as described below. Where we agree that the personal data is inaccurate or incomplete, we will try to tell any third party to whom we have disclosed the relevant data so that they can rectify the data, as well.

(iv) *Erasure*. that we erase the personal data we hold about you in the following circumstances:

(A) you believe that it is no longer necessary for us to hold the personal data we hold about you;

(B) we are processing the personal data we hold about you on the basis of your consent and you wish to withdraw your consent;

(C) we are processing the personal data we hold about you on the basis of our legitimate interest and you object to such processing. Please provide us with detail as to your reasoning so that we can assess whether there is an overriding interest for us to retain such personal data; or

(D) you believe the personal data we hold about you is being unlawfully processed by us.

Also note that you may exercise your right to restrict our processing of your personal data whilst we consider your request as described below. Please provide as much detail as possible on your reasons for the request to assist us in determining whether you have a valid basis for erasure. We will retain the personal data if there are valid grounds under law for us to do so (e.g., for the defence of legal claims or freedom of expression) but we will let you know if that is the case.

(v) *Restriction of Processing to Storage Only*: to require us to stop processing the personal data we hold about you other than for storage purposes in certain circumstances. Please note, however, that if we stop processing the personal data, we may use it again if there are valid grounds under Data Protection Law for us to do so (e.g. for the defence of legal claims or for another's protection). Where we agree to stop processing the personal data, we will try to tell any third party to whom we have disclosed the relevant personal data so that they can stop processing the data, as well. You may request that we stop processing and just store the personal data we hold about you where:

(A) you believe the personal data is not accurate, in which case processing will be stopped for the period it takes for us to verify whether the data is accurate;

(B) we wish to erase the personal data as the processing we are doing is unlawful but you want us to simply restrict the use of that data;

(C) we no longer need the personal data for the purposes of the processing but you require us to retain the data for the establishment, exercise or defence of legal claims; or

(D) you have objected to us processing personal data we hold about you on the basis of our legitimate interest and you wish us to stop processing the personal data whilst we determine whether there is an overriding interest in us retaining such personal data.

(vi) *Objection*: in certain circumstances, the right to restrict or object to our processing of your personal data (e.g. where you request correction or erasure, you also have

a right to restrict processing of your applicable data while your request is considered);

(vii) *Withdrawal of consent*: where you have provided personal data voluntarily, or otherwise consented to its use, the right to withdraw your consent; and

(viii) *Complaint*: the right to complain to the relevant supervisory authority.

(b) You may exercise the rights set out above by contacting the Data Protection Officer using the form available here or by emailing data-protection.officer@agilent.com. If you want more detail on when the rights apply, please contact the Data Protection Officer at the e-mail above. We must respond to a request by you to exercise those rights without undue delay and at least within one (1) month (although this may be extended by a further two (2) months in certain circumstances).

In the event that you wish to make a complaint about how we process your personal data, please use the above Data Protection Officer's email address and we will endeavour to deal with your request as soon as possible. This is without prejudice to your right to launch a claim the relevant data protection authority as stated at item (viii) above.

1.8 Your obligations in relation to Personal Data

Update Information

(a) It is important that changes in your personal circumstances are updated as soon as possible by either making the changes directly through the established process (currently Workday) or by contacting your local office Human Resources Department. These include changes to the following:

(i) name;

(ii) contact details (home address, phone number(s), email address(es));

(iii) marital status;

(iv) dependents (e.g. for private medical insurance purposes);

(v) emergency contacts and next of kin;

(vi) bank details for salary payment;

(vii) professional and educational qualifications;

(viii) languages, including levels of proficiency; and

(ix) tax code.

Hold data secure

(b) You may have access to personal data about other people and use this data in the course of carrying out your work duties. Under applicable Data Protection Laws, Agilent must

ensure that the personal data it holds about its customers, employees, suppliers or other third parties is held securely, not disclosed either orally, or in writing, or otherwise to any unauthorised third party and used only for appropriate purposes. You must take all reasonable steps to maintain the security of, and to keep confidential, all personal data held by Agilent to which you have access and you will use such personal data appropriately at all times. In particular, employee medical records must be kept separately from the employee's personnel file and should be accessible only by the company doctor and his medical staff, the HR Department (on a strict need-to-know basis), and the employee. Such records should be kept only for as long as is strictly necessary.

(c) Advice should be sought from Agilent's Information Security and Risk Management department when personal data is to be transmitted to any third party, including vendors.

(d) Any personal data or database accessed, compiled, generated, created, copied (in whole or part) by any employee in the course of their work is the sole property of Agilent, and may not be used or retained for any purpose other than Agilent business, in any circumstances. In particular, no part of any such database must be retained on termination of employment and must be delivered up, upon request, at any time (including when under suspension or on garden leave).

(e) Employees are responsible for the information they disclose and retain. If employees are in any doubt, or need to request any exception, they must consult their manager, or Agilent's Legal department, for appropriate guidance and approval.

Supplying or selling personal data

(f) Any employee who provides or sells, or receives any benefit from the supply of any Agilent personal data (i.e. including but not limited to data of employees, vendors, customers, prospects, partners) to any unauthorized third party, for any purpose, will commit a serious disciplinary offence (with sanctions up to and including termination of their employment); and will render themselves (and potentially also Agilent) liable to a criminal prosecution and a fine.

Breach of data security

(g) If you suspect a security incident has occurred or is about to occur, visit the Agilent ISRM CITSIRT webpage (https://spark.it.agilent.com/community/it-services/information-security), and contact CITSIRT immediately at CITSIRT@agilent.com.

For Employees, failure to comply with this Policy may result in disciplinary action up to and including dismissal without notice.

For Non-Agilent Workers, failure to comply with this policy may result in actions for breach of contract, up to and including actions for material breach of contract for third party contractors.

1.9 Related Policies

This policy should be read in conjunction with the following Agilent global policies: Agilent Acceptable Use Policies , Social Media Policy, Agilent Standards of Business Conduct; Sensitive Information Labeling Guidelines; Agilent's Document Retention Policies; and Agilent's Global Data Protection Impact Assessment Policy. Where there is a conflict between this policy and any other Agilent Policy then this policy shall prevail.

1.10 Changes to this Policy

This Policy may be amended from time to time at Agilent's discretion. This policy will be reviewed by Agilent's Chief Privacy Officer on an annual basis. You will be notified of any changes to these terms.

1.11 Local Law Requirements

Please refer to Appendix 2 to find out more information about the local law requirements that will apply in addition to the above, unless stated otherwise.

Appendix 1
Purposes for Processing Employee Data

Purpose of Use	Categories of Personal Data processed for each purpose	Legal Basis for Processing
HR Administration (Reporting): Compliance with all relevant legal, regulatory, governmental, mandatory and administrative obligations and responsibilities of the employer in relation to its role as your employer and in relation to your employment, whether such obligations and responsibilities are in the jurisdiction where you are based or elsewhere.	Contact details such as home and work address, phone numbers, email addresses, emergency contacts and next of kin information (name, contact number), date of birth, gender, compensation, tax unique identifiers, driver's license copies and/or driver's license numbers, National Insurance / social security number, employee ID number and health data.	Necessary for Agilent's legal obligations as an employer. Necessary for Agilent's legitimate interests (to comply with its responsibilities as an employer and to run a successful and efficient business).
HR Administration (Succession): Planning, consultative decision support and coaching.	Education details, employment details, gender, home and work address, and photograph.	Necessary for Agilent's legitimate interests (to comply with its responsibilities as an employer and to run a successful and efficient business).
HR Administration: Managing relocations, secondments, international assignments and work-related travel.	Employment details, compensation, employee ID and data related to travel and relocation (including address during any assignment/ secondment which requires relocation) for the purposes of the working relationship or as part of employee benefits programmes.	Necessary for Agilent's performance of the employment contract.
HR Administration (New hire on boarding): Administrative matters	Contact details such as home and work address, phone numbers, email addresses, date of birth, family details (such as contact details of spouse, partner and/or children),	Necessary for Agilent's legal obligations as an employer.

Purpose of Use	Categories of Personal Data processed for each purpose	Legal Basis for Processing
of on boarding new hires.	education details, employment details, compensation details, employee ID, social security number, tax unique identifiers, photograph, religious beliefs, trade union membership, political beliefs and health data (and in Denmark, criminal conviction data).	Necessary for Agilent's performance of the employment contract.
Training and development: Administration of training for required learning in relation to the employment.	Employee ID.	Necessary for Agilent's legitimate interests (to comply with its responsibilities as an employer and to run a successful and efficient business).
Benefits: Administration, management and execution of employee benefits, including expense benefits, health benefits, financial benefits and pension, retirement and life insurance schemes.	Contact details such as home and work address, phone numbers, email addresses, date of birth, employment details, gender, tax unique identifiers, National Insurance / social security number, bank account and payment details, employee ID, family details (such as contact details of spouse, partner and/or children), and health data.	Necessary for Agilent's performance of the employment contract. With the explicit consent of the data subject (where provision of data is voluntary). Necessary for Agilent's legal obligations as an employer.
Performance Management: Management of employees, including performance feedback.	Employment data including data with respect to the execution of the employment contract and continuing professional development such as secondments, training records, performance appraisals, career progression and promotions, and employee ID.	Necessary for Agilent's legitimate interests (to comply with its responsibilities as an employer and to run a successful and efficient business). Necessary for Agilent's performance of the employment contract.
Performance Management: Managing and reporting on disciplinary matters, grievances, queries and complaints, and	Data with respect to the execution of the employment contract including notes regarding discussions with Agilent management, performance appraisals and documents relating to complaints, grievances, disciplinary actions, promotions and demotions,	Necessary for Agilent's legitimate interests (to comply with its responsibilities as an employer and to run a successful and efficient business). Necessary for Agilent's performance of the employment contract.

Purpose of Use	Categories of Personal Data processed for each purpose	Legal Basis for Processing
corrective action for performance issues.	corrective action for performance issues, and employee ID.	
Termination: Administration of the termination of employment (both voluntary and involuntary) and to inform the other Group companies.	Contact details such as home and work address, phone numbers, email addresses, date of birth, family details (such as contact details of spouse, partner and or children), compensation, employment details, employee ID, and (in Italy) trade union membership.	Necessary for Agilent's performance of the employment contract. With the explicit consent of the data subject (where provision of data is voluntary).
Leave Management: Managing and reporting on sickness absence, occupational health services, maternity and paternity leave, paid and unpaid leave.	Contact details such as home and work address, phone numbers, email addresses, health data such as sickness days taken, employment details, employee ID number, compensation, family details (such as contact details of spouse partner and /or children), trade union membership.	Necessary for Agilent's performance of the employment contract. Necessary for Agilent's legal obligations as an employer. Necessary for Agilent's legal obligations as an employer.
Time & Pay: Time tracking and time keeping for the purposes of administering vacation leave and overtime.	Employment details and employee ID.	Necessary for Agilent's performance of the employment contract. Necessary for Agilent's legal obligations as an employer. Necessary for the performance of collective agreements.
Payroll: The administration of salaries, wages, bonuses and benefits, and the reimbursement of expenses.	Employment details, gender, compensation, bank account and payment details, employee ID, tax unique identifiers, National Insurance / social security number, contact details such as home and work address, phone numbers, email addresses, date of birth, trade union membership and religious beliefs (where relevant to religious tax reliefs applicable in certain jurisdictions).	Necessary for Agilent's performance of the employment contract.

Purpose of Use	Categories of Personal Data processed for each purpose	Legal Basis for Processing
Rewards and Recognition, and Incentive Pay: Annual rewards including rank, pay, compensation and bonuses; including local bonuses.	Employment details, compensation, employee ID, pay, bonus, social security number and work address.	Necessary for Agilent's legitimate interests (to comply with its responsibilities as an employer and to run a successful and efficient business). Necessary for Agilent's performance of the employment contract.
Physical Security: including Site Access management, issuing passes, CCTV monitoring and identification.	Employee name, address, photographs, email, video recordings.	Necessary for Agilent's legitimate interests (to comply with its responsibilities as an employer) and to provide a secure and safe work environment.
Information Technology: Administration of access, testing, support and security of IT systems for the use by employees and contractors	Employee ID, contact details, IP address of employee / NAWs computers and mobile device IDs. Additional personal data may be processed during the testing of IT systems where are dedicated to a particular purpose as explained in this table. For example, testing of a new HR system would involve the processing of personal data indicated in the 'HR Administration' above.	Necessary for Agilent's legitimate interests in providing access to IT systems, testing systems prior to roll out, support IT systems and maintaining security of IT systems for use by employees and contractors.
Distribution of Agilent Communications, Materials, Tools and Gifts: Including but not limited to distribution of legally required communications, sending of gifts,	Employee ID, contact details including name, email address, home address or alternative mailing address.	Necessary for Agilent's legitimate interests (including but not limited to the safeguarding of employee morale and connectivity) in communicating to employees, and ex-employees, from time to time, including the sending of legally required communications and documentation, sending of gifts or welcome kits, and other Agilent related

Purpose of Use	Categories of Personal Data processed for each purpose	Legal Basis for Processing
welcome kits to new employees, and other Agilent related documentation, tools and materials for approved business use.		documentation, tools and materials for approved business use.
Protect health and safety of Agilent employees from global health emergencies: including distribution of legally required communications, sending of health & safety supplies to employees, providing access to and facilitating health testing, and verifying where legally required vaccination status	Based on the nature of a global health emergency, and the legal requirements for an employee's country of residence, Agilent may collect: • Name(s) • Vaccination certificates • Information related to the employee's recovery from a particular health condition subject to the health emergency • Health testing results related to the health emergency condition	• Compliance with applicable regulatory obligations to protect the health and safety of Agilent employees, as applicable • Your express consent, if required under applicable laws

Appendix 2
Local Law Requirements

1. For employees in Norway:

(a) Control measures

If Agilent decides to implement measures that are considered to be "control measures" pursuant to the Norwegian Working Environment Act chapter nine, such measures will be carried out in compliance with the procedures and requirements stated in applicable law.

This implies that Agilent will only implement control measures that are objectively justified by circumstances relating to Agilent and provided it does not involve undue strain on the employees.

Agilent will, as soon as possible, discuss the needs, means and implementation of control measures and major changes to control measures with the employees' elected representatives.

Further, we will inform all affected employees with information on:

(i) the purpose of the control measures;
(ii) practical consequences of the control measures, including how the control measures will be implemented; and
(iii) the assumed duration of the control measures.

Agilent will, together with the employees' elected representatives, regularly evaluate the need for the control measures implemented.

(b) Deletion/closing of email accounts

Email accounts will be closed after the employment is terminated.

We will delete all emails, documents etc. stored on your personal area in the company's network and electronic devices made available to you by Agilent within a reasonable period after the employment has been terminated, unless such documents are necessary for Agilent's business.

(c) Video surveillance

Video surveillance at the Agilent work place will be carried out in accordance with the requirements and procedures in applicable Norwegian data protection law.

Agilent will only carry out video surveillance if there is a need to prevent hazardous situations and to safeguard the employees and others security or if there is a specific need for such surveillance.

We will make use of signs or other measures to ensure that you are made aware of the areas that are being kept under surveillance.

Video surveillance footage or other data collected through video surveillance will only be disclosed to other parties if:

(i) you have consented to such disclosure
(ii) disclosure is made to the police in connection with investigations of legal offences or accidents (unless such disclosure is prohibited due to statutory confidentiality obligations); or
(iii) if we are obliged by law to disclose the footage.

We will delete all video footage within a week after the footage is made. If it is likely that the footage will be disclosed to the police, we may keep the footage for a longer period of maximum 30 days. We may also store the footage for a longer period if you have consented to a longer storage period or we have grounds for storing the footage for a longer period pursuant to applicable data protection law.

(d) Records of personal injuries

Agilent is obliged to keep records of all personal injuries occurring during the performance or work and diseases assumed to have been caused by the work or by conditions at the workplace pursuant to the Norwegian Working Environment Act.

We will only keep records of medical information of a personal nature unless you have consented to this. We will treat the information as confidential information.

On request, we are obliged to make the records available to the Labour Inspection Authority, safety representatives, occupational health services and the working environment committee.

We are obliged to keep a statistical record of absence due to sickness and absence due to a sick child pursuant to detailed guidelines issued by the Directorate of Labour and Welfare, cf. section 25-2, first paragraph, of the National Insurance Act.

(e) Collection of health information and medical examinations

During the application and hiring process, we will only request for or in another manner obtain health information to the extent this is necessary for the performance of the work position.

We will only request that medical examinations of employees and job applicants are carried out if:

(i) we have a statutory obligation to do so
(ii) the working position involves particularly high risks
(iii) if we find it necessary to protect life or health.

2. For employees in Austria:

Due to Agilent's international corporate structure, the corporate group's matrix organization sometimes requires the establishment of a temporary or permanent international department. As a consequence, employees of AT Osterreich GmbH joining such departments are functionally bound to instructions by a superior employed by another member of the Agilent group. Notwithstanding such international

functional reporting lines, the employment relationship remains at any time with AT Osterreich GmbH. In case of any conflict of instructions, the instruction of AT Osterreich GmbH shall prevail.

3. For employees in Italy:

(a) Data Subjects' rights

In addition to the abovementioned rights, under Italian law, you are entitled to obtain (a) the anonymization of your personal data and (b) the certification that the operations related to your requests have been notified, as also relate to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected.

(b) Deadline to reply

In compliance with local requirements, Agilent will respond to a request by you to exercise those rights without undue delay and at least within fifteen (15) days (although this may be extended by a further fifteen (15) days in certain circumstances).

4. For employees in France:

(a) Data Subjects' rights

In addition to the above mentioned rights, for employees in France, please also note that you have the right to give us instructions regarding the retention, deletion and communication of your personal data after your death.