

## **DANAHER CORPORATION**

### **ASSOCIATE DATA PRIVACY NOTICE**

*Effective January 2, 2018*

#### **I. INTRODUCTION**

Danaher Corporation (including its direct and indirect subsidiaries) (“**Danaher**”) acts as a data controller with respect to the collection, use, and other processing of certain Personal Data about employees, whom Danaher refers to as associates (“**Associate Data**”) regarding the employment relationship, as described in more detail below. Associate Data is processed and included in a personal data file controlled by Danaher for the purpose of managing the employer/associate relationship.

#### **II. DEFINITIONS**

\* **Personal Data:** Any information that identifies an Individual or for which there is a reasonable basis to believe the information can be used to identify an Individual.

\* **Sensitive Personal Data:** Personal Data (i) about an Individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or criminal charges or convictions; (ii) that concerns health or sexual orientation; or (iii) that includes an Individual’s bank or credit card number, or any number that can lead to identity theft, such as a social security number.

#### **III. CATEGORIES OF ASSOCIATE DATA**

Danaher collects and processes the following Associate Data elements:

\* **Personal identification and family information:** associate’s name and contact information (home address, telephone and fax numbers and email address) and emergency contact information, gender, photograph (with associate consent), credit card and bank account details, and marital status. Where applicable, the following information about associate’s dependents: date of birth, nationality and residency information, social security or national insurance number or other local equivalent, identity card number, passport number, driver’s license

number, work permit number, tax identification numbers, and

\* **Personal employment related information,** including job/position title, supervisors’ names, titles and department, managers’ direct reports, work contact information (e.g., building location and address, telephone and fax numbers and email address), badge number, job reason code, job action code, region, time zone, associate identification number, IP address, username(s), password(s), access control data, CCTV data, division, subdivision, department, employment contract, employment history (including references from previous employers), expatriated status, working time, leave entitlements, salary and compensation related data (bonus information, pay scale and any salary-related changes), stock option and pension plan participation information, absence information, travel and expense related information, corporate credit card information, information on charges and deductions for payroll purposes (e.g., loans, alimony), Danaher property on loan, allowance information (housing, vehicle, transportation, meal, family or other), qualifications and professional experience, training, information regarding talent management, performance-related information and information relating to professional objectives, hire date, seniority date, departure date (where applicable), reports from executive search or employment firms (where applicable), and any additional information contained in conflict of interest certification statements.

Danaher also collects, processes and uses the following categories of Sensitive Associate Data to the extent legally permitted: social security number (or similar identifier), criminal history, drug test (Pass/Fail), ethnicity, race, veteran status.

#### **IV. PURPOSES OF PROCESSING OF ASSOCIATE DATA**

\* To the extent permitted under applicable data protection and local employment laws, Danaher collects, uses, and processes Associate Data for (a) the performance and the administration of your employment contract) (b) for compliance with a legal obligation of Danaher or (c) for Danaher's legitimate interests in running its business. The following are detailed purposes, where relevant to your role:

- \* administer current associate relationships (including workflow management and training of personnel)
- \* compensation and benefits (including stock plan administration and compensation and bonus analysis and administration)
- \* financial transactions (including payroll processing, management of salaries, expenses, taxes, required notifications to governmental authorities, assigning corporate credit cards and travel and expense reimbursement);
- \* recruitment (including job grading);
- \* maintaining associate directories and organizational charts;
- \* employee performance (including complaints / reports of misconduct, manage conflicts of interest, conduct performance appraisals, support career or leadership development, manage whistleblower program, customer interaction/satisfaction);
- \* security of Danaher assets and personnel (review video surveillance (e.g. CCTV) systems, review online behaviour, employee location, review email (during an investigation), review use of electronic asset-tools);
- \* workforce planning;
- \* employee engagement;
- \* brand promotion, maintenance and promotion of products/services (including marketing and social media activities);
- \* investigate instances of noncompliance with the law & corporate policies and manage disciplinary actions governance, monitoring and enforcing compliance with Danaher policies and procedures and with legal and regulatory requirements);

- \* IT administration (including providing IT support and services);
- \* Employee Health and Safety
- \* fraud/loss prevention and detection;
- \* mergers, acquisitions and/or restructuring (including completing any actual or proposed purchase of all or part of the business of Danaher or, in the case of any merger, acquisition or public offering, making available the necessary information to the purchaser of shares or assets of Danaher Corporation or any direct or indirect subsidiary thereof); and completing any other purposes directly related to those listed above.

A limited number of individuals within the HR, legal, finance and accounting and IT departments, as well as certain managers (i.e., persons with assigned responsibility or managerial responsibility for the associate or groups of associates) will receive access to specific and relevant Associate Data when necessary in connection with their job responsibilities.

Other third parties referred to in Section IV of this Notice may also collect, use, and otherwise process Associate Data for the fulfilment of all or some of the purposes stated in this Section IV and, in particular, in connection with the purposes set out in Sections V and VI, as applicable.

Other than for Danaher, Danaher does not collect, use, disclose, or otherwise process Associate Data for purposes of direct marketing. Subject to applicable law, Danaher will retain Personal Data no longer than is necessary to carry out the purposes listed in this Notice.

## **V. DISCLOSURES OF ASSOCIATE DATA TO THIRD PARTY SERVICE PROVIDERS AND INTERNATIONAL TRANSFERS**

As part of normal business operations, Danaher may disclose Associate Data to third party service providers for HR and payroll-related tasks (e.g., banks, insurance companies and other associate benefit providers), as well as governance, risk, compliance and security management. Danaher may also disclose Associate Data to third party service providers, for example in connection with information technology support (e.g., software maintenance and data hosting, remote management of IT infrastructure and applications, development and maintenance of applications and global service desk operations) and HR support (e.g., benefits and human capital management consulting, performance and talent management, career planning, associate training, payroll solutions and expense reporting, and credit card management), marketing and social media support, and in connection with corporate finance, accounting, reporting, and payroll services entrusted to such providers. In addition, for booking employment related travel arrangements, Associate Data may also be made available to a third-party travel agent, that, in turn, may transfer Associate Data to Danaher.

Some such third-party service providers may be located in territories outside of the EU that do not provide a level of protection to Personal Data equivalent to that provided by your home country. Danaher will (i) exercise appropriate due diligence in the selection of such third-party service providers, and (ii) require appropriate contractual measures, that such third-party service providers maintain adequate technical and organizational security measures in compliance with applicable legal requirements, in order to safeguard the Associate Data, and process the Associate Data only as instructed by Danaher and for no other purposes.

To provide adequate protection for the transfers out of the EU, Danaher utilizes transfer mechanisms recognized by your home country, which may include executing appropriate contractual clauses based on and conforming to the EU model clauses (the Danaher Data Protection Addendum). For more information on exactly how a transfer is protected, and to obtain a copy of the transfer mechanism, please contact your platform privacy leader.

Danaher may also disclose Associate Data to governmental agencies and regulators (e.g., tax authorities), social organizations (e.g., the social security administration), benefits providers (e.g., health insurers), external advisors (e.g., lawyers, accountants, and auditors), courts and other tribunals, and government authorities, to the extent required or permitted by applicable legal obligations.

## **VI. INTERNATIONAL TRANSFERS OF ASSOCIATE DATA WITHIN THE GROUP**

Shared Services Centres (SSC) are used for primary and back-up support depending on the region, and are responsible for carrying out certain administrative (e.g., HR, finance, payroll) functions on behalf of Danaher. Danaher and its third-party service providers may transfer Associate Data to the SSC. Danaher will ensure that steps are taken that are designed to provide adequate protection in respect of such transfers.

Danaher, its affiliated companies and the SSC may transfer Associate Data to Danaher Corporation located at in the United States, where Associate Data is protected in accordance with EU model clauses through the Danaher Global Data Protection Agreement.

Associate Data may be provided to authorized individuals (specifically, associate supervisors) through associate directories, use of personnel management tools, business applications, and regarding information technology support and business continuity/disaster recovery requirements. Associates with questions regarding affiliate companies of Danaher should contact their legal or privacy contact (SEE Section VIII). Danaher has implemented appropriate safeguards with its affiliated companies to protect disclosures of Associate Data.

## **VII. RIGHTS YOU MAY HAVE**

Associates have the right to access, transfer, object, cancel, review, update, correct and request the deletion or restriction of their own Associate Data in accordance with applicable law. These rights may be limited in some situations; as if it is determined to be infeasible to fulfill your request due a legal requirement. Also, associates are responsible for informing Danaher if there are any changes or inaccuracies to their Associate Data. Associates should submit any requests for access or updates to, or corrections or deletions of their own Associate Data to Danaher as specified below in Section VIII.

## **VIII. QUESTIONS ABOUT PROCESSING OF ASSOCIATE DATA**

Associates who have any questions about this Notice or wish to (i) access, transfer, object, cancel, review, correct or request the deletion or restriction of their Associate Data or learn more about who has access to such information, (ii) make any other type of request, or (iii) report a concern related to Associate Data, should contact their HR leader. While Danaher hopes it can answer any questions that associates may have, if you have unresolved concerns you also have the right to contact your local Data Protection Authority.

Your Platform Privacy Leader can be contacted for any additional inquiries about the Processing of your Personal Data.