HYKS-INSTITUUTTI

PRIVACY NOTICE REGARDING HR MANAGEMENT AND PAYROLL ADMINISTRATION
Updated on 19 May 2021

1. **Data Controller**
   Clinical Research Institute Helsinki University Central Hospital Ltd (business ID: 0872967–2)
   Mannerheimintie 105, PO Box 710, 00029 HUS, Finland

   ("**Clinical Research Institute HUCH**", "**we**", "**Data Controller**")

2. **Data Controller's contact person**
   Minna Aromäki, Financial Manager
   Mannerheimintie 105, PO Box 710, 00029 HUS, Finland
   ext-minna.aromaki[at]hus.fi

   The contact person is responsible for ensuring that Clinical Research Institute HUCH plans and carries out data processing activities in compliance with applicable provisions and decrees and works together with HUS Data Protection Officer.

   The Data Protection Officer of HUS acts as the Data Protection Officer:

   HUS Keskuskirjaamo
   PO Box 200, 00029 HUS, Finland
   eutietosuoja[at]hus.fi

3. **General**
   In this privacy notice we will provide information on how we process the personal data of our employees and officers as well as job applicants (the "**Data Subjects**"). We will also describe on what grounds and to what extent we process personal data. What has been stated in this privacy notice with respect to the processing of the personal data of our employees who are in an employment relationship with us will also apply to the processing of the personal data of people who are in a service relationship with us or who are applying for jobs.

   The provisions of the generally applicable EU General Data Protection Regulation (2016/679, the "**GDPR**") and the Finnish Data Protection Act (1050/2018) apply to the processing of our employees' personal data together with other applicable special acts, including the Finnish Act on the Protection of Privacy in Working Life (759/2004) and the Finnish Act on Electronic Communications Services (917/2014) (jointly the "**Applicable Legislation**").

4. **Purpose of and legal basis for the processing of personal data**
   We process personal data for the purposes of managing employment-related matters concerning the personnel of the Clinical Research Institute HUCH, such as determining the content and the terms and conditions of the employment, organising the employer's other obligations, such as occupational health care, monitoring working time and absences as well as taking care of matters related to the termination of employment and communication with the employees. The personal data of Data Subjects is processed particularly for the following purposes:

- Recruitment;
- Managing and supervising employees, including the management and supervision of working duties, planning staff roster, career development and promotions, measures related to the termination of employment, and planning and management of staff training;
- Up-to-date management of personal data as well as information related to the employment and salaries during the employment for the administration of employment-related matters and payroll and for filing the necessary information regarding terminated employment relationships;
- Fulfilling statutory obligations set out e.g. in labour laws, insurance laws and tax laws as well as reporting to the authorities and responding to the authorities' information requests or other requests;
- Ensuring that the instructions provided by the employer are followed and investigating cases of suspected misconduct;
- Managing work equipment, ensuring occupational safety and access control;
- Communication to employees and third parties, such as current or potential business partners, clients or suppliers.

The processing of personal data must be based on a legal basis set out in the GDPR. We process personal data on the basis of the following grounds, depending on the processing activity:

- Employment agreement concluded between the Clinical Research Institute HUCH and the Data Subject;
- Mandatory legislation;
- Data Subject's consent pursuant to applicable legislation; or
- The legitimate interest of the Clinical Research Institute HUCH or any third party (such as current or potential business partners, service providers or clients).

Examples of legitimate interest include e.g. ensuring and developing the safety of the premises, data security and data network security; protection of the Clinical Research Institute HUCH's property; prevention and investigation of frauds and abuse of the data systems and equipment that the Clinical Research Institute HUCH has provided to its employees; as well as internal investigation regarding suspected cases of abuse, offence or crime.

5. Personal data we process

We may process the following personal data that is directly necessary for the administration of our employees' employment and which relates to the management of the rights and obligations of the parties to the employment contract or to the benefits we offer to our employees or which we must process due to the special characteristics of our employees' work duties:

- **Basic information**, such as first and last name, home address, date of birth, personal identity code, sex, personnel number, contact details for close kin, phone number, e-mail address;

- **Basic information that relates to the employee's employment (and recruitment as applicable)**, such as their job application and other information relating to the application process (e.g. language skills), start and end date of the employment, employment contract and its terms and conditions, work duties and title, information related to insuring the employee, information regarding the termination of the employee's employment and letters of recommendation;
- **Information regarding salary payments and other compensation**, such as banking details, salary and other remuneration and benefits, information regarding work trips, travel time and destinations, information regarding taxes and employer contributions;
- **Information regarding work duties, work performance, professional development and work time tracking**, such as information regarding performance reviews, positions of trust, annual holidays and other agreed-upon absences (e.g. study leave and sabbatical leave);
- **Information regarding aptitude for work**, such as competence and training, personality tests and aptitude assessments, criminal record or credit record data to the extent that the Applicable Legislation allows or requires the processing of such data;
- **Information regarding equipment used by the employee**, such as the employee's email address and phone numbers, information regarding the access rights, user names and passwords granted to the employee for the purposes of accessing Clinical Research Institute HUCH's digital systems and registers, the identifying information of the equipment provided to the employee, such as computers, mobile terminals and access cards, keys and other corresponding equipment;
- **Data collected through technical surveillance systems**, such as Clinical Research Institute HUCH's system access logs, building access data and access surveillance recordings as well as video surveillance data and video surveillance recordings.

In addition, we may also process information regarding changes made to all of the categories of personal data that are disclosed above.

In addition to the personal data referred to above, we may also process certain special categories of personal data, i.e. sensitive data, as follows:

- **Information regarding union membership**, e.g. to enable us to pay union dues;
- **Information regarding our employees' health**, such as absences due to illness, but only to the extent allowed by the Applicable legislation for the following purposes: administration and payment of compensation, labour management (e.g. planning staff roster if employees are absent due to illness) and compliance with Applicable legislation and employment-related requirements as well as any doctor's notes or statements regarding employees or other information regarding an employee's health or ability to work in special cases to the extent that the processing of this kind of data is specifically provided for in the Finnish Act on the Protection of Privacy in Working Life or in other Applicable Legislation;
- **Information regarding work accidents**, to the extent that the processing of such data is allowed or required by Applicable Legislation, for the administration and payment of compensation (e.g. insurance compensation) and in order to ensure compliance with Applicable Legislation and employment-related requirements (e.g. occupational safety, reporting obligations);

- **Information regarding parental leave and partial care leave**, for the purposes of managing the workforce and to fulfil the requirements set out in Applicable Legislation; or
- **Drug test certificates** or the information disclosed therein to the extent that the Applicable Legislation allows for the processing of such data in order to assess the relevant employee's capability to work or function.

Please note that the employee's obligation to disclose personal data is partially statutory and partially based on the employment contract the employee has concluded with Clinical Research Institute HUCH. Refusing to disclose personal data may prevent us from carrying out some of the duties and obligations that relate to your employment, which may then result in the termination of your employment contract.

6. Regular sources of data

In accordance with the Finnish Act on the Protection of Privacy in Working Life, personal data concerning the Data Subject will be primarily collected from the Data Subject themselves at the beginning of and during their employment. Data will also be collected e.g. from systems that record information processed in connection with HR management and payroll administration (logs) and from other approved sources, such as the employee's supervisor, relevant public authorities (e.g. the Finnish Tax Administration, the Social Insurance Institution of Finland [Kela], enforcement authorities), other third parties (e.g. occupational health service providers) and/or from public sources in accordance with the Applicable Legislation. The Data Controller may also acquire the Data Subject's personal credit record or criminal record in order to assess their reliability. The Data Subject will be notified in advance if the Data Controller intends to acquire personal data regarding the Data Subject for the purposes of assessing the Data Subject's reliability.

7. Regular disclosure of personal data

Based on a separate assignment, we may transfer personal data to third parties that provide us with services, such as payroll administration services, IT or software services or other information processing services, for processing purposes. We have concluded a data processing agreement that meets the requirements established in the GDPR with all third parties that process personal data in order to ensure that all personal data is processed in accordance with the law.

The personal data of Data Subjects can also be disclosed to public authorities or to other third parties pursuant to Applicable Legislation or any decisions or orders handed down by a court of law or a public authority that are binding upon us. Personal data will be regularly disclosed e.g. to the Finnish Tax Administration, insurance companies, the Social Insurance Institution of Finland (Kela), pension institutions, occupational health service providers and trade unions.

Personal data can also be disclosed to the parent company as well as to the receiving organisation and its advisors with regard to transferring personnel in connection with a transfer of business that is conducted in accordance with the applicable business transfer provisions.

Personal data will not be disclosed to third parties for marketing purposes.

8. Retention period

We retain our employees' personal data in accordance with the Applicable Legislation only for as long as is necessary in order to implement the purposes for which the personal data is processed. Once the personal data is no longer necessary, the data will be destroyed or irreversibly anonymised.

The aforementioned does not, however, apply to personal data that is subject to a statutory retention period that is binding upon us. Personal data that is processed during an employee's employment is subject to several statutory retention obligations that we must adhere to as the employer. For example, basic information regarding the employee and their employment must be retained for a period of 10 years after the employee's employment has ended for the purposes of issuing letters of recommendation.

Any personal data of our employees that is exempt from the aforementioned statutory retention periods will primarily be deleted after 10 years have elapsed from the date on which the employee's employment ended. Our general, non-binding retention period for job applicants' personal data is one year from the date on which the recruitment decision is made.

9. Transfers of data to countries outside the EU or the EEA

In the event that we transfer personal data to a country that is located outside the EU or the EEA, we will ensure that the personal data will be processed in a manner that ensures an adequate level of data protection by concluding agreements or by implementing other appropriate safeguards. You can request additional information on cross-border transfers of personal data and the appropriate safeguards that apply to each specific transfer by contacting the contact person referred to above in section 2.

10. Principles for the protection of personal data

All personal data is processed with the level of care required by the GDPR and all data is protected appropriately. Personal data can be accessed only by persons who require access to the data in order to carry out their work duties.

The physical and digital security of the data that is stored electronically or manually is ensured by limiting access to the data only to those persons who are entitled to process the said data due to the nature of their work duties. These persons are subject to a confidentiality obligation. Digitally processed data is stored in databases that are protected with passwords, firewalls and other technical measures. All manually processed personal data is stored in a locked space to which access is limited. All materials will be destroyed in a manner that ensures the security of the data.

11. Data Subject's Rights

As a Data Subject you have the following rights related to the processing of your personal data under the GDPR:

- The right to obtain information on the processing of your personal data;
- The right to have access to your own information and to review your personal data;
- The right to request rectification of inaccurate or erroneous data and supplementation related thereto;

- The right to request the erasure of your personal data;
- The right to withdraw your consent and object the processing of your personal data to the extent the processing is based on your consent;
- The right to object the processing of your personal data on the grounds of your personal special occasion to the extent your personal data is being processed on the basis of the legitimate interest of the Data Controller;
- The right to receive your personal data in a machine-readable form and to transfer this data to another Data Controller provided that you have personally given this personal data to the Data Controller, the Data Controller processes this personal data on the grounds of an agreement and the consent provided by the Data Subject and processing will be carried out automatically; and
- The right to request restrictions on the processing of your personal data.

You may exercise the above-mentioned rights by sending a written request by mail or email to the contact person referred to in section 2. You may freely draft your own request or submit the enclosed form. If necessary, we may request you to specify your request and confirm your identity before we process your request. As a rule, we provide our answer to your request within one month from the date of accepting the request. Please note that your request cannot necessarily be processed if the GDPR provides grounds for the refusal.

12. The right to file a complaint to the supervisory authority

If you hold that the GDPR has not been complied when processing your personal data you have the right to file a complaint to the supervisory authority in that Member State where you hold a permanent place of residence or work position or where the claimed infringement of rights has occurred.

In Finland, the applicable supervisory authority is the Finnish Data Protection Ombudsman:

The Office of the Finnish Data Protection Ombudsman
PO Box 800, 00531 Helsinki, Finland
tietosuoja[at]om.fi
https://tietosuoja.fi

HYKS-INSTITUUTTI

APPENDIX

Please submit the form to:
Clinical Research Institute
HUCH
PO Box 710
00029 HUS, Finland
ext-minna.aromaki[at]hus.fi

With this form, I can execute the rights related to the processing of my personal data.

I wish to: **(Please choose one or several options depending on which rights you wish to exercise)**

☐ obtain information on the processing of my personal data;

☐ have access to my own information and to review my personal data;

☐ request rectification of inaccurate and/or erroneous data and/or supplementation related thereto;

☐ request the erasure of my personal data;

☐ withdraw my consent and object the processing of my personal data to the extent the data processing is based on my consent;

☐ object the processing of my personal data on the grounds of my personal special occasion to the extent my personal data is being processed on the basis of your legitimate interest;

☐ request restrictions on the processing of my personal data.

A further specification of how I wish to use my rights and on which my request is based:

_____

_____

_____

_____

_____

By signing this form, I confirm the choice I have made above.

Contact details (used only for the purposes of executing my rights)

Full name:

Personal identity code (or date of birth if you do not have the code):

Street address:

Postal code and post office:

Email:

Place and date:

Signature: