Speak-Up Channel Privacy Notice

Introduction

This Speak-Up Channel Privacy Notice explains how Celltrion Europe Entities (the "Company" or "We") processes personal data within the Speak-Up Channel, which allows stakeholders to report misconduct or concerns. The Speak-Up process aims to gather evidence, take appropriate action, and protect you as a "Reporter".

Your personal data will be processed only to the extent necessary for the Company to comply with (EU) 2016 the "General Data Protection Regulation" (GDPR) and any applicable law, and under this Notice. Where an individual Member State's law imposes additional requirements, which are more stringent or stricter than those imposed by this Notice, the requirements in the Member State's law must be followed. Furthermore, where a Member State's law imposes a requirement that is not addressed in this Notice, the relevant Member State's law must be adhered to.

Categories of Data Processed

The type of data processed may vary depending on the nature of the reported incident. The following categories of data may be processed:

1) Data of Reporter

To ensure that the reporting individual remains anonymous, the following mandatory information will not be allowed for identifying the Reporter. However, on a voluntary basis, you as a Reporter may provide contact information, such as personal data or an email address, to receive notifications from the Company regarding the progress of their Report.

- Contact Information: Name, Email address
- Relationship to Celltrion Europe Entities: This may include categories such as employee, former employee, prospective employee, contractor, supplier, etc.
- Report Key: Used for case retrieval and communication with the Global Compliance Division

If you have provided your personal data including your contact details, we will follow up and inform you about the status of the investigation, to the extent that this is requested and/or permitted under the Company's Speak-Up Channel Policy.

2) Content of Reported Incident

- Description of the reported compliance breach
- Activities related to Celltrion Europe Entities (Celltrion Healthcare Hungary, Celltrion Healthcare UK, Celltrion Healthcare Ireland, Celltrion Healthcare Germany, Celltrion Healthcare France, Celltrion Healthcare Italy, Celltrion Healthcare Belgium, Celltrion Healthcare Netherlands, Celltrion Healthcare Finland, Celltrion Healthcare Romania, Celltrion Healthcare Czech Republic, Celltrion Healthcare Austria, Celltrion Healthcare Norway, Celltrion Healthcare Denmark, Celltrion Healthcare Poland, Celltrion Healthcare Switzerland)
- Location and time of the incident
- Any other relevant information necessary for investigation

- Technical Data:
  - Session cookies for reports via the web portal
  - Voice recordings for telephone reports

3) Data of Person Subject to Incident Reporting

- Contact Details: Name, Job title, Address, Email address, Phone number, Company, and Country
- Content of the Reported Incident:
  - Description of the behavior or activities related to Celltrion Healthcare European Entities
  - Any other data pertinent to the allegation
- Measures Taken: Actions or corrective measures implemented in response to the reported incident (if applicable)

Access to and disclosure of personal data

Personal data will be processed in accordance with and on the basis of the Reporter's consent given when reporting via the Speak-Up channel. By submitting Report via the Speak-Up Channel, you give the Company to 'process' and 'transfer' collected Personal Data under this Notice.

Only the investigation team of that Report has right to direct access to personal data. If necessary, personal data from Reports may be transferred to other group companies of Celltrion. This is the case if the reported cases are processed on behalf of these group companies, an employee of the company, or a supplier or other partner of this Company. If necessary, personal data will also be transferred to competent state authorities, such as investigative authorities. The Company will take appropriate measures, in compliance with applicable law, to ensure that your personal information remains protected.

Data storage periods and data deletion

The Company adheres to the statutory retention periods as mandated by the respective legislation of the country of the commissioning Group company.

Personal data contained in the incident report will be processed for the maximum duration permitted by the applicable laws and regulations, provided that such data remains relevant for the investigation. This retention period may be extended if the investigation is ongoing until the case is resolved.

- Case data will be anonymized as soon as possible after the case closure
- Voice recordings will be deleted as soon as possible after transcript/summary confirmation

Upon the expiration of all retention periods, the data will be deleted in compliance with data protection regulations. Any personal data will be removed once it is no longer necessary to fulfill legal obligations.

Please refer to the Company's Data Retention & Erasure Policy for full details on our retention, storage, periods and destruction processes.

Rights of the Data Subjects

Under GDPR, you have rights regarding your personal data, including the right to confirmation and access to your processed data (Article 15), rectification of incorrect data (Article 16), erasure of your data (Article 17), restriction of processing (Article 18), data portability (Article 20), and objection to processing (Article 21).

However, these rights may be limited in specific circumstances per GDPR. Additionally, the identities of

incident subject remain confidential when exercising these rights, and he or she will be informed of allegations after the initial investigation to ensure proper defense.

If you would like to exercise any of these rights, please contact the Company's Data Protection Officer (please refer to 'Contact Us' section below)

International Transfers of Data

To the extent that this is necessary for us to carry out the tasks described in our Speak-Up Channel Policy, we may transfer information related to the Reports to Celltrion, Inc. which is the Celltrion Headquarter located in Republic of Korea. We may only transfer your data if there is a legal basis for the data transfer.

On 17 December 2021, the European Commission (the Commission) and on 23 November 2022, the Information Commissioner's Office (the ICO) each adopted an adequacy decision for South Korea. This means that free unrestricted transfers of personal data from the European Economic Area (EEA) and/or the UK to private and public entities in South Korea will be permitted from that date onwards (including remote access from South Korea) without the need for certain restrictions such as, but not limited to, implementation of Standard Contractual Clauses.

Changes to this Privacy Notice

This Privacy Notice may be changed by us unilaterally from time to time, in particular, if we change our data processing or in case of new legislation. Please refer often to this page for the latest information and the effective date of any changes. The version published on this website is the current version.

All inquiries about this Notice, including requests for exceptions or changes should be directed to the Data Protection Officer (Please refer to 'Contact Us' section below)

Contact Us

If you have any specific questions, if you would like to exercise your right to access, rectification, deletion/erasure, object, restrict processing or portability, or if you want to file a complaint, please contact us at:

- DPO: dpo.cthc@celltrionhc.com

- Country Designated DPO (if applicable)
  - ✓ Germany:
    - Name: DDI (Deutsches Datenschutz Institut GmbH)
    - Email: ulrike-alexandra.seitzinger@deutsches-datenschutz-institut.de
  - ✓ France:
    - Name: Elise Dufour
    - Email: dpo.cthc.fr@celltrionhc.com
  - ✓ Italy:
    - Name: Felic Cuzzilla (DWF Italy)
    - Email: Felice.Cuzzilla@dwf.law
  - ✓ UK, Belgium, Finland, Netherlands, Irelands, Hungary:
    - Name: Privaon (Gail Maunula, Andrill Konopko)
    - Email: info@privaon.com, andrill.konopko@privaon.com, gail.maunula@privaon.com

Also, you may lodge a complaint with the relevant supervisory authority if you consider that our processing of your personal data infringes applicable law. Please refer to Appendix A for Contact details for EU Supervisory Authorities.

CELLTRION

Appendix A - Table of relevant EU Data Protection Laws & EU Regulatory Authorities

Country	Local Data Protection Law	Regulatory Authority
Italy	(EU) 2016 the "General Data Protection Regulation" (GDPR) The "Privacy Code".	Garante per la protezione dei dati personali. (the "Garante"). Piazza Venezia 11 - 00187 Roma. Phone: +39 06.696771. Email: protocollo@gpdp.it
UK	(EU) 2016 the "General Data Protection Regulation" (GDPR) Data Protection Act 2018. The Privacy Electronic Communications (EC Directive) Regulations 2003.	Information Commissioner's Office. ("ICO"). Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF. Phone: 0303 123 1113.
Ireland	(EU) 2016 the "General Data Protection Regulation" (GDPR). The Irish Data Protection Act 2018.	Data Protection Commission. ("DPC"). 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland. https://www.dataprotection.ie/en/contact/how-contact-us
Germany	(EU) 2016 the "General Data Protection Regulation" (GDPR). German Federal Data Protection Act (Bundesdatenschutzgesetz – 'BDSG')	The Hessian Representative for Data Protection & Freedom of Information. PO Box 3163, 65021 Wiesbaden. https://datenschutz.hessen.de/service/besch werde
France	(EU) 2016 the "General Data Protection Regulation" (GDPR). The French Data Protection Act. French ePrivacy Directive 2002/58/EC.	Commission Nationale de l'Informatique et des Libertés. ("CNIL") 3 Place de Fontenoy TSA 80715 75334 Paris CEDEX 07. France. Phone: +33 (0)1.53.73.22.22.
Netherlands	(EU) 2016 the "General Data Protection Regulation" (GDPR). The Dutch GDPR Implementation Act (Uitvoeringswet AVG, the Implementation Act.	The Dutch Data Protection Authority. Autoriteit Persoonsgegevens PO Box 93374, 2509 Aj Den Haag. Phone: (+31) - (0)70 - 888 85 00
Belgium	(EU) 2016 the "General Data Protection Regulation" (GDPR). 'Data Protection Act' of July 30, 2018	Autorité de protection des données Gegevensbeschermingsautoriteit. The Data Protection Authority. Rue de la presse 35, 1000 Brussels. Phone: +32 (0)2 274 48 00 Email: contact@apd-gba.be https://www.dataprotectionauthority.be/contact-us

Finland	(EU) 2016 the "General Data Protection Regulation" (GDPR). Act on Electronic Communication Services 917/2014 'Data Protection Act 2019'.	Office of the Data Protection Ombudsman. ("Tietosuojavaltuutetun Toimisto") Postal address: P.O. Box 800, 00531 Helsinki, Finland. E-mail: tietosuoja(at)om.fi
Hungary	(EU) 2016 the "General Data Protection Regulation" (GDPR).	Hungarian National Authority for Data Protection & Freedom of Information. (Nemzeti Adatvédelmi és Információszabadság Hatóság) H-1125 Budapest, Szilágyi Erzsébet fasor 22/C. Phone: +36 -1-391-1400 E-mail: privacy@naih.hu