Information on data protection

With this web-based whistleblowing system (hereinafter, the **"DQ System"**) FUJIFILM Holdings Corporation (hereinafter, **"FH"** or **"we"** or **"us"** or **"our"**) provides a means for reporting specific compliance violations concerning all of our direct and indirect subsidiaries (jointly with us the "**Fujifilm Companies**"), branches and our and their employees. The processing of personal data in the DQ System is based on the legitimate interest of Fujifilm Companies located in Europe, the Middle East and Africa to detect and prevent misconduct in our group, and thus to avoid damaging Fujifilm Companies, their employees and customers.

We take data protection and confidentiality very seriously and adhere to the provisions of the EU General Data Protection Regulation (hereinafter, the **"EU-GDPR"**) as well as current national data protection regulations and other laws governing the operation of a whistleblowing system. The following will explain the handling of personal data that may be included in reports submitted by you via the DQ System. Personal data means any information that identifies a person or at least makes a person identifiable, such as an email address, a phone number, a job title, location data, etc.

Responsible party and technical maintenance

The party responsible for the use of the DQ System and for processing the reports within the Fujifilm group is FUJIFILM Holdings Corporation, 7-3, Akasaka 9-Chome, Minato-ku, Tokyo, 107-0052, Japan.

Technical operation and maintenance of the DQ System is performed by a third party, D-Quest, Inc. of 12F Ryumeikan-honten Bldg., 3-4 Kandasurugadai, Chiyoda-ku, Tokyo, 101-0062 Japan (hereinafter, **"DQ"**), on behalf of FH. Personal data and information entered into the DQ System are stored in a database operated in a high-security data center in the EU. All data is encrypted, pseudonymised and password-protected. It is then transferred to DQ's two Japanese servers, where it is further encrypted, and ultimately stored in DQ's report server. FH is then notified by DQ of the existence of a report.

Confidential handling of reports

Incoming reports submitted by you are handled by a small circle of expressly authorized and specially-trained employees from the CP&RM (Compliance and Risk Management) Group of FH ESG (Environment, Social and Governance) Division (hereinafter, **"FH's CP&RM Group"**) in a strictly confidential manner. Before data is transferred to FH's CP&RM Group, a German law Firm retained by DQ will pseudonymise all reports by deleting any personal data. Only based on such pseudonymised reports, FH CP&RM Group will evaluate the matter, perform further internal investigations, if required, and, if necessary, involve other FH Corporate Divisions (such as HR, Legal or Accounting) and relevant FH subsidiaries. Generally, FH's CP&RM Group will only be able to contact the relevant whistleblower and receive relevant contact information if the whistleblower decides to share such information. FH CP&RM might have access to further personal data of the involved individuals mentioned in the report.

During processing of a report or internal investigation, it may become necessary to share reports with additional employees, divisions of FH subsidiaries or external investigation specialists. All persons involved in these activities are either subject to professional secrecy or bound to confidentiality by appropriate contractual arrangements.

Sharing information with recipients outside the EU/EEA

In order to conduct or complete internal investigations, personal data that you have provided in your report may be transferred to Fujifilm Companies or third parties outside the European Union (hereinafter, the **"EU"**) or the European Economic Area (hereinafter, the **"EEA"**) – specifically, Japan. As the European Commission decided that Japan ensures an adequate level of personal-data protection, effective as of January 2019, your personal data may be transferred between the EU, EEA and Japan without having to implement additional safeguards usually required for transfers to third countries. If there are any material changes regarding the processing locations, we shall duly inform you of such changes without undue delay and implement the necessary safeguards to ensure your data is kept secure.

Access of government agencies

FH may also be required by law to provide government agencies or courts with information about compliance violations. In this case, as well as in the event of loss or confiscations of company assets, we might not be able to withhold the information provided by you.

Types of collected personal data

Use of the DQ System takes place on a voluntary basis. There is no statutory or contractual obligation for you to use the DQ System unless otherwise specified. If you submit a report via the DQ System, the following personal data and information might be collected and processed:

- your name, if you choose to reveal your identity (which in some jurisdictions is mandatory, in which case it will be indicated to you when you use the DQ System),
- your email address, your company name, your position, if you choose to reveal them, and
- the names of persons and other persons' personal data that you name and describe in your report.

Information of the incriminated person

As a basic principle, we are bound by law to inform the incriminated person that we have received a report concerning him or her. As such information can potentially jeopardize our ability to effectively investigate the allegation, the information to the incriminated individual may be delayed as long as such risk exists. However, if you have disclosed your identity there maybe situations where the incriminated person shall be informed about your identity by concerned authorities or by us when instructed to do so by an authority.

Rights of the data subjects

According to the EU-GDPR, you and the persons named in the report have the right to access, rectification, erasure, restriction of processing and the right to object to processing of personal data concerned. Further, you have the right to lodge a complaint with a competent supervisory authority in accordance with the applicable laws and regulations in case you have a concern about the processing of your personal data. For this purpose, you can contact the supervisory authority in the EU Member State of your habitual residence or the place of the alleged infringement.

However, the aforementioned rights may be restricted in order to ensure the protection of the whistleblower. Even if the whistleblower discloses his or her identity, the person accused in a whistleblower's report can under no circumstances obtain information from us about the whistleblower's identity on the basis of the accused person's right of access, only except where the whistleblower has maliciously made a false statement concerning the person accused. In all other cases, we guarantee the whistleblower's confidentiality to the utmost extent legally possible.

Retention period of personal data

We will at all times strive to accelerate our investigations of any alleged misconduct and complete such investigations as soon as reasonably possible. Personal data is only retained for as long as is necessary to clarify the situation and evaluate the report, a legitimate interest of FUJIFLM exists or it is required by law. After the report processing is concluded, this data is deleted in accordance with applicable statutory requirements.

Use of the reporting portal

Communication between your computer and the DQ System takes place via an encrypted internet connection (SSL). Your IP address will not be stored during your use of the reporting system. In order to maintain the connection between your computer and the DQ System, a cookie is stored on your computer that merely contains the session ID (a so-called null cookie). This null cookie is only valid until the end of your session and expires when you close your browser or switch off the device.

In case you would like to communicate with FH's CP&RM group, you will need to provide an e-mail address. Such e-mail address is kept confidential by DQ and only stored in the European data center used for the operation of the DQ System. The e-mail address will only be used for communication between you and the DQ System. The e-mail address will not be transferred by the DQ System to us, except with your prior consent. All communication between you and us will be indirectly through DQ and the DQ System. If you are a user in the EMEA region and you would like to remain fully anonymous, you must submit your report without providing an e-mail address. However, in such case, FH's CP&RM Group will not be able to provide any response to you, to ask questions or to otherwise communicate with you regarding the reported matter.

Consent and voluntary nature

By using this DQ System, you agree that your personal data, to the extent provided by you, will be collected, processed and used as described above. If you do not want FH to collect, process and use your personal data as described, you may submit your report anonymously to the extent permitted under applicable laws. The disclosure of your personal data is voluntary, as is the use of the DQ System.

We would, however, appreciate it if you state your full name and contact details, as many internal investigations can be facilitated if the name of the whistleblower is known.

Providing the personal data information as described above is not a statutory or contractual requirement, nor is it necessary for you to enter into contact with us, except as otherwise set out above. Failure on your part to provide the necessary data as described above when voluntarily using the DQ System may limit FH's effectiveness in investigating any claims brought forward by you via the DQ System.