26/09/2024

DRC's Code of Conduct Reporting Mechanism GDPR Statement

The security of your personal data is very important to Danish Refugee Council (the "**DRC**") and to the Safeguarding & Code of Conduct teams in particular (the "**SaG & CoC Team(s)**").

DRC's CoCRM Privacy Policy (the "**CoCRM Privacy Policy**") provides you with detailed information about how we collect, use and keep your personal information secure. We encourage you to read this CoCRM Privacy Policy carefully and if you have any questions or concerns about how DRC uses your personal data, please contact gdpr@drc.ngo and we will try to address your concerns.

I. Scope of the CoCRM GDPR Policy

This Privacy Policy applies to all personal data relating to your involvement in a report of suspected misconduct (the "**RSM**") lodged within DRC's Code of Conduct Reporting Mechanism (the "**CoCRM**").

Your involvement may be due to the fact that you have lodged yourself an RSM in the CoCRM, that you are mentioned in it in your quality as complainant (the "**Complainant**"), witness, subject of concern (the "**Subject**") or even that you are mentioned in this RSM without any specific quality, but that your name appears in the RSM.

It is therefore not linked to your employment with DRC or with your membership of DRC's Executive Committee.

II. What data do we collect?

We collect the information that are provided to us directly by the person reporting the RSM (the "**Reporting Person**"). We also collect information from our interlocutors in the frame of the processing of an RSM. This includes individuals but also other departments of DRC (e.g. Human resources) including departments from other DRC's operations and locations. This notably includes the information collected during internal investigations. We finally collect information that are publicly available (for example on internet, social media etc.).

The personal data we collect can be grouped into the following categories:

- Identity and background information: for example, name, phone numbers, as well as e-mail, postal and/or residential address, nationality, gender, , language, age
- Employment data: for example, type of employment agreement, seniority, job position, role description.
- Human capital information: for example, attended trainings, certifications, performance and learning dialogues, development needs, measures, and disciplinary actions.
- Special categories of personal data: for example, information concerning health, sexual orientation, ethnicity, disability, background checks.

Special categories of personal data are collected when they directly relate to the allegation reported to DRC's CoCRM and to DRC's CoCRM purpose.

III. What is the legal ground for processing your data?

We use and process your personal data based on the following legal basis:

- The processing is necessary for compliance with a legal obligation (e.g. whistleblower laws and regulations), or
- It is deemed to be a "legitimate interest" of the controller, company or third-party (e.g. proceeding with internal investigation relating to Code of Conduct misconduct, misuse of DRC assets and image, breach of contract and internal policies etc.), or
- You have consented to it.

IV. Who has access to your data?

As the privacy of individuals is of utmost importance to DRC, this Privacy Policy will be updated on an ongoing basis to make sure that we comply with legal requirements.

The data we collect and process is only accessible to the members of the Safeguarding & Code of Conduct teams as well as the members of DRC's personnel who are allowed to access these data as per DRC's CoCRM Operation Handbook (the "**CoCRM OH**").

The following person have therefore access to your data:

- The members of the Safeguarding & Code of Conduct Unit in HQ.
- The Regional Safeguarding & Code of Conduct Coordinators at Regional levels.
- The persons holding the role of registrar of the CoCRM (the "**Registrar(s)**").
- The persons holding the role of authorising officer (the "**Authorising Officer(s)**").
- The persons holding the role of Intake Committee members (the "**ICM(s)**").

All the above persons may only access your data after they have been formally appointed by the management in charge and after they have signed a confidentiality undertaking. All the above persons do not have the same access to your data. Their access is restricted to their specific tasks and roles as per DRC's CoCRM policies and operating procedures.

Managers and Human Resources Managers in charge of following up with an RSM may also be granted with access. This access is limited to the specific case file and report for which they are in charge of following-up. Reporting Person's and survivors' (the "**Survivors**") of Sexual exploitation, abuse or harassment (the "SEAH"), personal data may only be shared with management if they have consented to it.

V. How will we use your data?

Your data will be used for the purpose of the processing of RSMs in the frame of DRC's CoCRM, which includes the conduct of administrative internal investigations, and the prevention and response to Code of Conduct misconduct.

For more information about DRC's CoCRM purpose, see DRC's Code of Conduct here.

VI. How do we store your data?

Your data can be collected using physical documents such as the report form. However, your data is only stored in the Code of Conduct database (the "**CoC Data Base**"). All physical documents is immediately destroyed after your data has been registered on the CoC Data Base. This database is confidential, its access is restricted and only the following persons have access to it:

- The members of the Safeguarding & Code of Conduct Unit in HQ.
- The Regional Safeguarding & Code of Conduct staff at Regional levels.
- The persons holding the role of registrar of the CoCRM (the "**Registrar(s)**").
- The persons holding the role of authorising officer (the "**Authorising Officer(s)**").

While the Safeguarding & Code of Conduct Unit (HQ) has access to all data stored in the CoC Data Base, the regional Safeguarding & Code of Conduct staff have an access that is limited to cases affecting countries in their own regional area. The country Safeguarding & Code of Conduct Registrars have an access that is limited to cases affecting their own country only.

Your data is also stored in the RSMs' case files stored on CoCRM sharepoint. Investigators may only access the specific case file for which they have been formally appointed as an investigator. Other access rights to CoCRM sharepoint are handled the same way as for the CoC Data Base.

Specific IT support staff may be granted access for the purpose of their assignment in DRC. They are bound by a strict confidentiality agreement.

VII. How do we protect your data

We take the security of your personal data very seriously. We have implemented various strategies, controls, policies and measures to keep your data secure and keep these measures under close review. We protect your data by using encryption techniques and we use other safeguards such as firewalls and password protection. This means that your data is protected and only accessible by DRC employees who need it to carry out their job responsibilities. We also ensure that there are strict physical controls in our buildings which restricts access to your personal data to keep it safe.

In addition, all our communications containing personal data and made via email are encrypted manually. Reports on investigation are never shared via email but only via a link from the CoCRM Sharepoint in order to ensure that the IT protections in place in DRC also apply here.

VIII. How long do we store your data?

We will keep your data for as long as it is needed for the purposes for which your data was collected and processed or required by laws and regulations. This means that we keep your data for as long as necessary for the performance of our legal obligations, our obligation towards donors, auditors and for the purpose of the management, prevention of and response to Code of Conduct misconducts.

The retention of personal data in the CoC Data base is maximum 12 years, except otherwise provided by local applicable law. After 12 years, your name will be deleted from the case file in order to ensure anonymisation.

IX. What are your data protection rights?

You have the following rights:

Request access to your personal data. You have a right to access the personal data we are keeping about you. Your right to access may, however, be restricted by legislation, protection of other persons' privacy and consideration for DRC's business concept, business practices and investigation interests. DRC's know-how, business secrets as well as internal assessments and material may restrict your right of access.

Request correction of incorrect or incomplete data. If the data is incorrect or incomplete, you are entitled to have the data rectified, with the restrictions that follow from legislation.

Request erasure. You have the right to request erasure of your data in case:

- The data was collected based on your consent and you withdraw your consent to the processing and there is no other lawful basis for processing.
- You object to the processing and there is no justified reason for continuing the processing, processing is unlawful.

Limitation of processing of personal data. If you contest the correctness of the data which we have registered about you or the lawfulness of processing, or if you have objected to the processing of the data in accordance with your right to object, you may request us to restrict the processing of the data to storage only. The processing will only be restricted to storage, until the correctness of the data can be established, or it can be checked whether our legitimate interests override your interests. If you are not entitled to erasure of the data which we have registered about you, you may instead request that we restrict the processing of the data to storage only. If the processing of the data which we have registered about you is solely necessary to assert a legal claim, you may also demand that other processing of the data be restricted to storage. We may process your data for other purposes if this is necessary to assert a legal claim or if you have granted your consent to this.

Object to processing based on our legitimate interest. You can always object to the processing of personal data about you for direct marketing and profiling in connection with such marketing.

Data portability. You have a right to receive personal data that you have provided to us in a machine-readable format. This right applies to personal data processed by automated means only and on the lawful basis of consent or performance of a contract. Where secure and technically feasible the data can also be transmitted to another data controller by us.

Your request to exercise your rights as listed above will be assessed given the circumstances in the individual case. Please note that we may also retain and use your information as necessary to comply with legal obligations, resolve disputes and enforce our agreements.

If you wish to exercise your right to access your personal data, to object to it being processed or to rectify processed data, please contact gdpr@drc.ngo or send a letter to Danish Refugee Council, Borgergade 10, 3.sal, 1300 Copenhagen K, Denmark.

X. To whom may we disclose your data?

We may share your personal data with others such as authorities (if we have an obligation to do so or provided that it is authorised by law), DRC companies and entities, suppliers (for the sole purpose of the processing of your personal data on our behalf or for the purpose of an internal investigation).

If the above implies third country transfers, we may transfer personal data to organisations in so-called third countries (countries outside of the European Economic Area). Such transfers can be made if any of the following conditions apply:

- the EU Commission has decided that there is an adequate level of protection in the country in question, or
- other appropriate safeguards have been taken, for example the use of the standard contractual,
- safeguards in place, or
- that there are exceptions in special situations, such as to fulfil a contract with you or your consent to the specific transfer.

DRC is a global organization and personal data submitted or collected may be transferred to our various entities, divisions, joint ventures and affiliated companies around the world, located inside or outside the European Economic Area (EEA) for the purposes described above. An updated list of the DRC entities worldwide is published on a regular basis. The company overview can be found here. The level of protection afforded by the laws of the different countries may vary. However, DRC will make all reasonable efforts to ensure that processing of your personal data by DRC (or its agents) outside the EEA will be carried out in a way which provides equivalent protection to the standards applied by DRC within the EEA and that external data processors meet high data security standards to protect your personal data.

We may finally share your data to other NGO or donors provided that we have received your explicit and informed consent in order to allow them to review and proceed with investigations that are outside our own mandate.

XI. Contacts and Complaint

If you are unhappy with the way DRC processes your personal data, you can always contact the relevant Data Protection authorities in your country of residence if this is an EU membership country or the Danish Data Protection Authority in Denmark:

Datatilsynet
CVR nr.: 11883729
Adresse: Borgergade 28, 5., 1300 København K, Denmark
Telefon: +45 33 19 32 00
E-mail: dt@datatilsynet.dk