POLICY

24 MAJ 2018

Processing of personal data

- governing the Danish Red Cross association

Version 0.8
The policy was approval by the Governing Board on 7 June 2018

THIS POLICY INDICATES HOW WE MUST AND SHOULD PROCESS PERSONAL DATA ABOUT THOSE WE WORK FOR AND WORK WITH.

CONTENTS

1 INTRODUCTION

Everybody has the right for their personal data to be protected. Personal information or personal data range from name, address and pictures to social security number and religious beliefs. In the Red Cross we receive, store and use personal data on many people. It is important for the work and reputation of the Red Cross that all of these people can count on us to process their personal data according to current legislation[1].

The policy introduces a number of new concepts – appendix 1 gives you an overall view and show what the concepts mean. Below is a short introduction to the main concepts:

Personal data (information) is data making it possible to identify a person. In the Red Cross, personal data is typically name, contact information, email, etc., but may also be personal data of a more sensitive nature, such as health details.

Processing is everything we do with the personal data, i.e. when we collect, store, read, edit, search for and pass on data.

Protection is about every person's right to decide which personal data he/she wants to share – and who to share it with. When collecting personal data, that means that we have to use the data only for what we have agreed with the person. So, the people we process personal data on (**the data subjects**) must inform us how we may process their data.

2 PURPOSE AND RESPONSIBILITY

The purpose of this policy is to establish the scope for how personal data must and should be processed in the Red Cross and to give a reference to how to process the data.

The overall data responsibility for processing personal data in the Red Cross (data controller[2]) lies with the national Red Cross association (hereinafter 'Red Cross') and includes all processing of personal data in the Red Cross-national branches with associated activities and at the national office, including offices abroad, the psychosocial centre and the asylum department. In practice this means that the national office of the Secretary-General is data controller.

The Danish Red Cross Youth organization is considered an independent data controller, as they are an independent legal entity. The Danish Red Cross youth is thus responsible for their processing of personal data, and therefore they have their own personal data policy and guidelines.

This policy and the associated guidelines apply to everybody in the Red Cross processing personal data, i.e. both volunteers and employees. Employees means all managers and employees at Red Cross-national branches and at the national office, including employees in the asylum department, the psychosocial centre and delegates.

---

[1] Current legislation is the EU General Data Protection Regulation effective 25 May 2018 and supplementary Danish personal data protection laws. In everyday speech, the regulation is referred to as GDPR (General Data Protection Regulation).
[2] See definition in appendix 1.

The responsibility to work out and comply with the policy lies with the national office management consisting of the secretary general, the assistant secretary general, and the branch managers. Branch managers are charged with ensuring that the policy distributed to the volunteers and the employees who process personal data and to check compliance with the policy.
Sanctions for not complying with current legislation or leakage of personal data in the form of a fine or criticism from the supervisory authority is handled by the national Red Cross association as the overall data controller.

Data protection contact; is a person appointed from each Red Cross branch board of directors to keep a special eye on personal data and its processing and who may help the branch to ensure that the processing in the specific Red Cross branch complies with this policy and the associated guidelines.

Volunteers; must comply with the policy and associated guidelines as presented to them in the form of manuals and guidelines. If problems arise, the volunteer must discuss the issue with the data protection contact in his/her branch or the branch chairman and then contribute to act on the issue.

Employees; must be informed about and comply with the policy and the underlying guidelines. If uncertainties arise, the volunteer must discuss the issue with the immediate manager and then contribute to act on the issue.

The department head; must ensure that the employees are familiar with the policy and the underlying guidelines. If the employees, contrary to expectations, do not comply with the current guidelines, the head of department must take necessary measures to ensure the current guidelines are complied with pointing forward.

The Red Cross data protection officer (DPO[3]); must ensure that the Red Cross complies with the general data protection regulation and the present data protection policy.

Guidelines and practical instructions will be developed continuously for the compliance of the data protection policy by both employees and volunteers (see appendix 4). The data protection policy and guidelines will be published various places depending on which Red Cross unit you belong to, i.e. it may be at www.mitrødekors.dk or the Intranet at the asylum department, Branch Office Copenhagen or the national office. The policy will refer to the Intranet as a collective name for all units.

Questions about the policy or the guidelines that cannot be answered by your immediate manager or the data protection contact in the branch is sent to the DPO at DPO@rodekors.dk.

3 PROCESSING OF PERSONAL DATA

This section will explain the issues you must consider every time you plan to process personal data. Many of the processes performed at the Red Cross are described in guidelines and manuals, but you must also be able to assess if the planned processing complies with current rules.

If you are not sure if you are allowed to perform a process or if an ongoing process complies with the rules, it is important that you ask your immediate manager, the data protection contact or the DPO.

[3] DPO is short for Data Protection Officer. The Red Cross processes a large amount of sensitive personal data, and therefore the Red Cross must have a DPO according to the EU general data protection regulation.

3.1 Definition of personal data

As mentioned, personal data (information) is data making it possible to identify a person. A lot of information about a person is regarded as personal data. In the Red Cross, we process a large amount of ordinary and sensitive information. The difference between ordinary and sensitive personal data is that we must provide extra protection for sensitive personal data, e.g. there are additional requirements to processing security. Read more about processing security in section 5.

The table below shows which data are regarded as ordinary and which data are regarded as sensitive personal data.

Ordinary personal data	Name, address, work and private phone, mobile number, work area, email, IP address, title, employment date, CV, application, degree, car, residence, family matters, employment matters, sick days, debt, tax, finance, other purely private circumstances, essential social conditions
Sensitive personal data	Race, ethnicity, political, religious or philosophic beliefs, union membership, genetic data, biometric data for unambiguous identification, health details, sexual behaviour or orientation, convictions, offences, social security number and ID for an asylum seeker

Personal data may be a combination of data where each part does not identify a person, but the combination of data enables identification. For instance, it is not possible to identify a person based on the title 'branch chairman', but if it is combined with the branch name, the person can be identified, even though his/her name is not mentioned.

3.2 Lawfulness of processing (legal processing)

We are allowed to process all personal data which the Red Cross has a legitimate purpose to process, both ordinary and sensitive personal data – as long as lawfulness of processing applies. Lawfulness of processing is a legal concept indicating whether it is lawful to carry out a planned processing of personal data.

When you collect personal data in the Red Cross, it must thus be for a legitimate purpose, and you must ensure the processing is lawful, i.e. that lawfulness of processing applies.

Lawfulness of processing may be based on various factors deciding if a processing is lawful. The lawfulness of processing applying to the purpose is chosen for each processing instance. If there is no lawfulness of processing supporting what you want to achieve, the processing cannot be carried out.

You have lawfulness of processing (legitimate processing) when you

- Need to execute an agreement with the data subject (**contractual obligation**)
- Need to fulfil a legal obligation (**legislation**)
- Need to process personal data as part of the task that the Red Cross needs to perform (**legitimate interest**)
- Have **consent** from the person whose data you are processing
- Are in an emergency where you have to carry out the processing to protect the **vital interests** of the data subject or others
- Find that the processing is of **public interest**.

For instance, we need to know who the Red Cross members are. The purpose is to know who has voting rights in the association and who to collect membership fee from. To fulfil our purpose, we thus need to keep a record with contact information for all our members. Lawfulness of processing is based on legitimate interest, as the processing is part of the task that the Red Cross must perform. Thus, it is in our legitimate interest to register the data as long as the member wants to be a member.

See more information about the above-mentioned lawfulness of processing and examples of how to use it in appendix 2. Note that if you base lawfulness of processing on consent for the planned processing, the consent must fulfil a number of requirements.

Consent must be voluntary, specific, unambiguous and must be informed consent for the data subject to understand what is agreed to. A consent is invalid if it is impossible for the person to say no. The consent must be given at the time of collection, at the latest.

In general, it must be possible to document the consent. If it is necessary to use the consent in a process where it is not possible to document the consent, the process must be clarified in collaboration with the DPO before processing is initiated.

For more information on how to obtain and document consent, read 'Guidelines for obtaining consent'. Here there are also consent examples and a template to obtain consent. Find guidelines and the template on the Intranet.

Processes where we process personal data in the Red Cross are described in 'Records of processing activities' available on the Intranet. It also describes the overall processing purposes and lawfulness of processing.

3.3 How to do this

When you plan to process personal data, you need to consider a number of issues thoroughly before initiating the processing:

a. What is your purpose with the processing?
b. What personal data do you need?
c. What is lawfulness of processing based on?
d. Who needs access to the personal data you collect?
e. Where is the personal data to be stored?
f. For how long are the personal data you collect to be stored and when are they to be deleted?

When you start collecting personal data, you must remember that the people you process personal data about must be informed about the processing. Read more about the duty to disclose in section 3.4.

Example of the above process:

a. A volunteer in a Red Cross shop wants to make a birthday list of volunteers in the shop.
b. The volunteer needs the name and the birthday.
c. Lawfulness of processing requires the volunteer to ask the other volunteers if they would like to be on the list – so consent is obtained.
d. All volunteers working in the Red Cross shop
e. The list is posted on the notice board in the back of the shop.
f. The list is updated when new volunteers arrive or when someone stops working in the shop. Old lists are deleted electronically, and the printed version is destroyed.

When collecting names and birthdays of the volunteers in the shop, the volunteer informs that the list will be posted on the notice board in the back of the shop, that it can thus be seen by everybody entering the room and that they may be deleted from the list at any time, i.e. retract their consent.

When you collect data, you must ensure only to collect personal data you need. If you receive more information than needed, ask the person to limit the amount of data pointing forward and delete the unnecessary data.

Already when collecting personal data, you must consider how long time you need to store it. You must delete the data when the purpose of processing of the data has ceased, or when processing is no longer lawful. Read more about data deletion in section 3.6.

When storing data electronically, you must also consider who will have access to the data you process; if it concerns a list of participants at a family camp, only the people involved in organising it need to see the list of participants. It may seem rather innocent that a list of participants is shared with strangers, but if you see it from the perspective of the data subject, it is not certain that the data subject wants others to know that he/she has participated in a family camp.

It is important to be systematic when storing personal data to always know where the data is, in case the data subject asks to gain insight, wants to edit data or to have his/her personal data deleted. Sensitive or confidential information must be locked away or stored in a system with limited access. Only the persons who are to take part in the processing based on your considerations above may have access to the stored data.

So, we must always ensure that we consider the rights of the data subjects.

3.4 The rights of the data subjects

So, the purpose of the regulation is not to prevent us from processing personal data, but on the contrary, to ensure that the processing is lawful, is performed considering the rights of the data subjects, so that the data subjects are informed about how we process their personal data in an easily understood way.

The right of the data subjects to oversee their personal data is specified in six rights which the data subjects can use, i.e. the right to:

- Know that your personal data is being processed (duty to disclose)
- Know which personal data is registered (right of access)
- Have incorrect personal data corrected (right of correction)
- Have personal data deleted (right to be forgotten)
- Protest that personal data is used for direct marketing or profiling
- Transfer personal data to another organisation.

Overall, we accomplish the right to know that personal data is processed, i.e. the duty to disclose of the Red Cross, by having a privacy policy on our website, rodekors.dk, that you have to refer to in writing or verbally when you collect data.

If there are things the data subject needs to be told about the processing that is not included in the privacy policy, you must yourself inform the data subject about it. Regarding the above example with a volunteer wanting to make a birthday list of the volunteers in the shop, this birthday list is not mentioned in the privacy policy, as it is not possible to mention every processing of personal data in

the privacy policy. Therefore, the volunteers accepting to be on the list must be informed specifically about how their personal data is processed, i.e. as mentioned above, names and birthdays are written on a list which is posted in the back of the shop.

When a data subject inquires to have his/her data corrected, you must ensure that it happens, and that it happens everywhere the person's data is registered with us. The data subject may also ask to have his/her personal data deleted. If the data subject asks to have access to or to be deleted and you have doubts about how to do this, contact your immediate manager, the data protection contact in your branch or the DPO. Note that the Red Cross only has one month to correct or delete data from the date when the data subject requests it. Read more about data deletion in section 3.6.

When a data subject asks for access, they have right of access to all the information that you and others in the Red Cross have registered for that person. Therefore, it is important you do not save personal data that you do not have lawfulness of processing for.

If a person request to have his or her personal data moved to another organisation and you have doubts about how to do this, contact the DPO.

3.5 Processing of human resource data

At the Red Cross, we process personal data about employees and applicants to jobs and volunteer jobs.

Regarding employees, the legal framework for the processing is that we have concluded an agreement. What the processing specifically includes and how it is carried out is specified in the Red Cross 'privacy policy for processing of personal data on employees'.

Regarding volunteers, the legal framework for the processing is that we have concluded a Red Cross agreement. What the processing specifically includes and how it is carried out is specified in the Red Cross 'privacy policy' available at www.rodekors.dk.

If employees receive an application and a CV outside the Red Cross human resource systems for handling applicants, these must always be forwarded to human resources who will ensure correct processing of the personal data of the applicant. Received applications and CVs may not be kept for more than six months, unless consent is given for it.

Information received from applicants to volunteer jobs may not be kept for more than six months, unless consent is given for it.

3.6 Deletion of personal data

As mentioned, you may only save personal data as long as the processing is legal and is carried out according to the original purpose. When you no longer have a valid reason to keep the data, they must be deleted.

If you need to keep data for statistics, e.g. about how many families participated in an activity, and how many children the family has, you can choose the make the list anonymous by removing all information enabling us to identify the data subject. Then the list consists of an anonymous designation, e.g. family 1 with three children, family 2 with one child, etc. The important part of the anonymization is being aware that in a certain context, a combination of information may still lead to the

identification of a person, even though the name and contact information is removed. If this is the case, more data needs to be made anonymous, to make is legal to store the data.

If a person asks to have his/her personal data deleted, the personal data of this person must be deleted in all systems, emails and physical folders where that person is registered. But the person cannot be deleted if the registration is lawful according to the law or to the fulfilment of a contract.

For people registered more than one place or in several systems, it can be a huge exercise to delete that person's data, as he/she may be registered in several Red Cross branches and at the national office. If you have doubts about how to perform the task, ask your manager or the DPO. Note that the Red Cross only has one month to complete this task.

Remember that printed documents with sensitive personal data must be destroyed in a proper manner, e.g. by shredding.

Please note that the Red Cross has made an agreement with the National Archives on handing over historical data. If you have doubts about which historical data must be handed over to the National Archives, ask the DPO.

3.7 Use of pictures and video

At the Red Cross, we use pictures and video to communicate on websites, mitrødekors.dk, social media, leaflets, presentations, etc.

A picture or a video is regarded as personal data if it is possible to identify just one person in the picture or the video, and with that, the use of the picture or video is subject to the rules of processing of personal data.

That means we must ensure there is a specific purpose and lawfulness for using the picture or video before we start. In 'Guidelines for using pictures and video', you can read how to make sure you can use the picture or video. You can find these guidelines on the Intranet.

3.8 Transfers to third countries

The regulation includes strict rules on when personal data can be processed outside the EU/EEA[4] and how it must be carried out. The purpose is to ensure that personal data only is shared outside the EU/EEA if the same level of security can be obtained when processing personal data as if the processing took place inside the EU/EEA. Transfers to countries outside the EU/EEA are referred to as third-country transfers.

In the Red Cross, we continuously share personal data with delegates, other Red Cross organisations, partners, donors, etc. across borders. When it comes to so-called safe countries outside the EU/EEA, we must make the same considerations as with any other processing of personal data inside the EU/EEA; we must consider the purpose of the processing and whether we have legal basis for completing the processing. There are only a few countries outside the EU/EEA considered as safe countries, e.g. Switzerland[5]. Note that the U.S. and Australia are not currently considered safe countries.

---

[4] The EEA is an economic co-operation between the EU and Norway, Iceland and Liechtenstein.
[5] The European Commission is continuously reconsidering which countries are safe. At the moment, these third countries are classified as being safe: Andorra, Argentina, the Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay.

If you need to transfer personal data to so-called unsafe third countries, i.e. outside the EU/EEA, first read 'Guidelines for third-country transfers' on the Intranet. This document shows if the required processing is legal. The same goes when you want to transfer personal data from a third country to the EU/EEA.

If the processing of personal data does not involve an EU citizen and the exchange of data is between two countries outside the EU/EEA, the regulation does not apply to this transfer. For ethical reasons, the Red Cross will always try to ensure that the processing of personal data about non-EU citizens outside the EU/EEA is carried out as safely as possible. However, the conditions under which the Red Cross are working, e.g. a disaster scenario, must be weighed against the need to protect personal data in the situation at hand.

4 AGREEMENTS WITH SUPPLIERS PROCESSING PERSONAL DATA

We must enter an agreement with all suppliers processing personal data for the Red Cross, a so-called data processor contract. This contract must be entered in addition to the main agreement with the supplier. Typically, such a supplier will be an IT supplier, but it may also be a telemarketing agency or local authorities. The purpose of entering into a data processor contract is to instruct the data processor in what they can do with the personal data they process on our behalf.

When you enter into a contract with a new supplier processing personal data, you must also ensure that a data processor contract is made.

There are a number of requirements as to what a data processor contract must include. In 'Instructions on data processor contracts', you can read more about the process of entering into data processor contracts, what information the contract must include, and how we then monitor the contracts. On the Intranet, you can find templates in Danish and English for data processor contracts. Note that the DPO must always perform quality assurance on data processor contracts before they are signed.

5 SECURITY OF PROCESSING

In the Red Cross, the processing of personal data is subject to our 'Information security policy' which indicates how information is classified in the Red Cross, and what that means to the data processing. Appendix 3 gives you a quick overview of the classification. The purpose of the classification is to assist volunteers and employees in handling data correctly according to current legislation and internal guidelines.

It is the responsibility of the service owner[6] to ensure that the systems they are responsible for meet these requirements.

As mentioned, additional demands are made to the security of the processing of sensitive personal data, such as social security number and health details. Such data may only be shared by email if a Red Cross email is used. If sharing sensitive personal data is part of the task, volunteers must therefore have a Red Cross email before the task is performed[7].

---

[6] Service owner is a department manager responsible for an IT system. In the asylum department, the term system owner is used.

[7] All Red Cross volunteers are offered to have a Red Cross email address, also volunteers not processing sensitive personal data. If you are a volunteer and want a Red Cross email address, send an email to helpdesk@rodekors.dk.

If sensitive data is sent to an external person, e.g. an authority, the email must be sent as 'Secure email', which encrypts the information and reduces the risk of strangers gaining access to the data considerably. You can see instructions on how to send secure email on the Intranet.

The Red Cross are not allowed to ask the data subject to send e.g. a social security number by email to the Red Cross, but if the person chooses to do so, it is at his/her own risk.

You may not share confidential personal or business data through systems which the Red Cross is not able to control the access to and which does not comply with the password policy, cf. the classification of data in the data security policy. Examples of such systems are Dropbox or Google Drive.

If unauthorised persons have gained access to personal data of a data subject, the Red Cross is required to report the security breach to the Danish Data Protection Agency and the data subjects within 72 hours of discovering the breach. Therefore, a volunteer or employee who becomes aware of unauthorised access to personal data, either externally or internally, must report it at once to his/her immediate manager and the DPO.

Appendix 1: DEFINITIONS

Below are definitions of selected terms used in the main text.

Personal data (information)
Personal data enabling a person to be identified, directly or indirectly, alone or in combination.
The difference between ordinary and sensitive personal data is that we must provide extra protection for sensitive personal data, e.g. there are additional requirements to processing security. Read more about processing security in section 5.

Ordinary personal data	Name, address, work and private phone, mobile number, work area, email, IP address, title, employment date, CV, application, degree, car, residence, family matters, employment matters, sick days, debt, tax, finance, other purely private circumstances, essential social conditions
Sensitive personal data	Race, ethnicity, political, religious or philosophic beliefs, union membership, genetic data, biometric data for unambiguous identification, health details, sexual behaviour or orientation, convictions, offences, and social security number

Processing
Any activity or series of activities involving the use of personal data, i.e. to view, read, collect, register, organise, store, search for, use, pass on or delete.

Data subjects
All the people we register personal data on.

Protection
Everybody as the right to decide which personal data he/she wants to share – and who to share it with – unless something else provides lawfulness of processing, e.g. legislation demanding that income is reported to the tax authorities. When collecting personal data, that means we must use the data only for what we have agreed with the person. So, the people we process personal data on (**the data subjects**) must inform us how we may process their data (duty to disclose).
The regulation makes stringent demands for processing personal data in the sensitive personal data category. The security for the processing of personal data is shown in section 5.

Lawfulness of processing
Lawfulness of processing is a legal concept indicating whether it is lawful to carry out a planned processing of personal data. Appendix 2 contains examples of lawfulness of processing.

Duty to disclose
The duty to tell the data subject how we process his/her personal data. The data subject can read about how the Red Cross processes personal data at www.rodekors.dk under 'privacy policy'.

Data controller
The person responsible for how data is processed in the Red Cross, i.e. the person deciding which purpose we base the processing of personal data on and which tools we use.

Data processor
The supplier or public authority processing personal data on behalf of the data controller.
Record of processing activities

The record is the way the Red Cross documents to the Danish Data Protection Agency which personal data we process and how it is done. The record replaces the notification obligation to the Danish Data Protection Agency required by the former Danish Data Protection Act. You can find an overview of the records and all the records on the Intranet.

The EU data protection regulation
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Danish data protection act
The act expected to be passed based on the bill on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (data protection act) introduced on 25 October 2017.

Appendix 2: EXAMPLES OF USE OF LAWFULNESS OF PROCESSING

Below are examples of how lawfulness of processing is determined and what kind of processing we can then perform. Lawfulness of processing is a legal concept indicating whether it is lawful to carry out a planned processing of personal data.

Execute an agreement with the data subject (contractually obligated)
A contractual obligation can be a contract with a supplier, a Red Cross agreement with a volunteer, or an employment contract. When a contract is signed, we have the right to process the personal data in the contract until the contract expires.

If a volunteer does not want to be a Red Cross volunteer anymore, it is not legal for us to process that person's data unless another lawfulness applies. If a volunteer is e.g. a contributor, we are obligated to store the person's data for five years according to the Danish Bookkeeping Act. You may also be obligated to delete a person's information in one location while you must keep it in another location.

A donor agreement is also a contractual obligation, and such an agreement can require for personal data to be saved for up to seven years after the last payment to enable the Red Cross to document what donations are used for.

Fulfil a legal obligation (legislation)
We are obligated to processing personal data according to other legislation besides the data protection regulation. The Danish Health Act e.g. requires medical records to be saved for ten years, which includes e.g. health clinics and the ambulance service. The Red Cross is also obligated to report paid wages to the Danish tax authorities and to book income and expenditure even though it involves processing of personal data.

The data subject cannot reject data processing required by legislation. Note that even though we are bound by law to process personal data with the purpose to obey the law, we do not have the right to use the data for any other purpose.

Process personal data based to the legitimate interest of the Red Cross
Legitimate interest deals with a data processing necessary for completing a task in the interest of the Red Cross. An example is when registering members. If we were not allowed to register members, the member would not be able to vote at the general assembly and we would not be able to collect the membership fee. Thus, it is in our legitimate interest to register the data as long as the member wants to be a member.

Another example is the distribution of Christmas support (for low-income families). It is completely legitimate for us to register who has applied for Christmas support, so that we on the day know who to give the Christmas support to. But we cannot subsequently use the list of Christmas support recipients to send an invitation to participate in another activity. If you want to inform Christmas support recipients about other Red Cross offers, you have to do it at the same time as handing out the Christmas support.

It is legitimate for us to register collectors in the national collection; how else are we to know who will be collecting on the day. It is also of legitimate interest to ask collectors from last year if they want to collect again. But if more than three years have passed since a collector has collected, there is no longer a connection to the Red Cross that allows you to ask again.

Consent
Consent is used when we have no other lawfulness for the data processing we want to complete.

Consent is used when we want to use a picture of an identifiable person on our website or some other form of communication. You can read more about using pictures in Guidelines for using pictures and video.

Consent is also used if you are in contact with a group of people in one context and you want to contact them in another context. For instance, if you want to contact Christmas support recipients when planning a family camp. Then you can ask for their consent to contact them when you send invitations to the family camp. Read more about consent in section 3.5.

Vital interest
This lawfulness may only be used in a few instances, such as if a first-aider is to treat an unconscious person and it is not possible to ask for consent for processing of personal data.

Public interest
There are only a few instances where lawfulness of processing of personal data may be based on 'public interest'. An example could be research of such a nature that public interest overshadows the rights of the data subjects. This lawfulness may only be used if it is specifically indicated as the lawfulness for processing in the records of processing activities in the guidelines for this policy or as specifically agreed with the DPO.

Appendix 3: DATA CLASSIFICATION IN THE RED CROSS

Category	Types	
	Business data	*Private data*
Public There is no confidentiality and no limitation to who can have access	No business-critical data For instance, published accounts and information about the Red Cross, which may be found on the website, etc.	If the material contains personal data, you must be authorised to publishing these (through legislation, contract, or consent). Examples include pictures on the website and personal stories in leaflets.
Internal Information concerning all or certain volunteers and/or employees, but not the public	Business data not currently to be shared outside the organisation. Examples include internal email, memos, and reports	If personal data is registered or shared, you must be authorised to do so (through legislation, contract, or consent). An example is registering personal data in databases.
Confidential Data only concerning a few selected volunteers and/or employees in the Red Cross that others are not allowed to access	Business-critical data Examples include internal email, memos, and reports with a high degree of confidentiality	If sensitive personal data is registered or shared, you must be authorised to do so (through legislation, contract, or consent). Examples include sensitive information about participants in activities and projects, volunteers and employees (social security number, health, religious and financial information, race and ethnicity, etc.)

Appendix 4: OUTLINE OF INSTRUCTIONS

Below are the guidelines as mentioned in this Policy.

- Guidelines for using pictures and video
- Guidelines for obtaining consent
- Guidelines for third-country transfers
- Guidelines for obtaining data processor contracts
- Guidelines for volunteers processing personal data are included in manuals for activities and other relevant instructions