CISV International
Building global friendship

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

DATA PROTECTION MINI-GUIDE

DATA PROTECTION– KEY POINTS

This document is a summary of some key points that you may find of interest. It is not complete and it gives a simple introduction to what are often complex matters; it is not legal advice and is meant only as help notes for staff and volunteers.

Advice and Responsible Person

Please check your national and local laws, as the General Data Protection Regulation (GDPR) might be carried out or understood differently in different countries. You also might have additional local or national laws that you need to follow.

This is a complex area and we recommend that someone (preferably several people if possible) in each NA and Chapter is responsible for learning about data protection, staying informed, and providing general advice to your boards on any actions to take. There are probably trainings available in your country that you could use. There are some general links for guidance on the legislation at the end of this document.

What does Data Protection Demand or Seek to Achieve?

- ✓ Protect the privacy of individuals
- ✓ Justify the use of personal data
- ✓ Keep it safe and accessible only to those who need it
- ✓ Limit the amount of personal data organizations hold and keep it accurate
- ✓ Give it only to those who need it
- ✓ Get rid of it when you don't need it

What information does Data Protection apply to?

Data protection applies to all personal data that is collected or used by an organization.

It does not apply to personal data that:

- Each of us uses only for personal or household activities
- Has been completely anonymised

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

What is Personal Data?

Personal data is data that relates to a living and identified, or identifiable, individual.

- It can be concrete, e.g. name, address, ID number
- Or subjective, e.g. opinions that someone in the organization has recorded about a person or that person's choices or behaviour

It may include special categories of more sensitive data e.g. health, religion, philosophical beliefs. We are required to take extra care with sensitive data. We are also required to take extra care with children's data and we must have parental consent to use most children's data. (This is why we ask for parental consent on our Legal Forms).

Data Protection rules are based on 7 Principles

1. Lawfulness, Fairness and Transparency

Lawfulness * – there must be a clear reason for us to use the data
Fairness – we must use data in a way that is reasonable and does not discriminate against individuals or groups
Transparency – we must explain to people how we will use their data
*There are 6 possible reasons that can make it lawful for us to use data. The most relevant for CISV are the last two, consent and legitimate interest. When it comes to sensitive data, there are additional rules in local and national laws, that you should make sure to check.

- Legal Obligation – for example, an employer must provide employee data to the tax authorities
- Official Authority or Public Interest – when an organization is legally allowed, but does not have to do something, e.g. local authorities can collect tax payers' details
- Vital Interests -- for life and death situations, when we need to use data to address a direct and immediate threat to life
- Necessary for a Contract – this may apply when there is a contract between the individual and the organization, e.g. it is given as a reason in the system we use to register people for the Global Conference; there, we have to process the data in order to enable that person to participate in the Global Conference. If you are a Chapter with a written agreement between the Chapter and families for participating in programmes this could also be relevant.
- Legitimate Interest – Generally, this is something that an organization wants to do, but it may not be 100% necessary for the organization to do it. This is where as an organization, when we use data, we have to balance the benefit to CISV with the impact on the person and that person's expectations.

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

Notes on Lawfulness, Fairness and Transparency:

- Legitimate interest is not likely to be accepted as a good reason to keep personal data, if the benefit to the organization is minor while there is a high negative impact on the person. If an organization wants to use this reason it has to be on the basis of a documented impact assessment. The organization then takes full responsibility for the judgement and decision.
- You do not need someone's consent to use their data if there is a true and acceptable legitimate interest. However, it can be helpful to use 'opt-outs' - You are then saying that we think it is important for us to use your data and we have a legitimate interest to do so, but we give you the chance to opt out. If someone opts out, we must not use or share their data.

- Consent – This is where it is the individual who decides if we may use their data. The person has to have a genuine choice in the matter and their consent must be freely given. Their consent must be very clear and you must be able to show that they gave consent. For us to be able to rely on consent, the person has to "opt-in".

Notes on consent:

- If you are going to make consent to something a condition of participating in or getting a service, it can only be consent to something that is necessary to the activity/service they have agreed to or have paid for. E.g. you can buy something in a store without them sending you marketing material in the future, so they can't make you give consent to receive marketing as a requirement for making the purchase.
- If you wish to use data that is special category data, then you will need the person's explicit (written) consent. An important exception is where there are vital interests (life and death) at stake and the person is incapable of giving you their consent to use their data, e.g. emergency medical information

2. Purpose limitation – we must have a clear and defined lawful purpose to use the data and we only use the data for that purpose

3. Data minimization – we only use the data we need to run our organization, and where possible we make it anonymous or make it difficult to identify the person for instance.

4. Accuracy –we must make an effort to keep accurate information, so we avoid problems such as mistaken identity.

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

5. Storage limitation – the length of time that we store data should be in accord with the purpose for which the data is held. (see below)

6. Integrity and Confidentiality – we must take every effort to keep data secure, such as use technical safeguards (like firewalls and encrypting laptops) and take organizational steps (like training people on use of passwords) to make sure the data is safe.

7. Accountability – As a data controller organization, CISV is responsible for, and must be able to demonstrate how we comply with, the above 6 Principles.

Storing Personal Data

You must keep personal data in a way that is confidential and secure.

This means that only people who need access to it should have access to it. You must make sure that you:

- Keep paper documents in secure / locked areas.
- Password protect electronic data and the computer you held it on. (see next section)
- Consider extra security (Encryption) for your computer and for confidential or sensitive data (e.g. financial, ID, health).
- Use secure memory sticks for backups or travel or to send data.

Sending Personal Data

When you send data, you must make sure it is only sent to persons/email addresses you know and trust.

You should consider when you need to encrypt data files. You can encrypt files with 7-zip (http://www.7-zip.org/). It is free to use. You can create secure passwords at https://passwordsgenerator.net/ - passwords should never be easy to guess!

You must send the encrypted file and the password separately, preferably via different media – e.g. send the file via e-mail, and the password via text message – or at least send the file and password in two different e-mails at different times.

If your email is sent between addresses with Transport Layer Security (TLS) and between known recipients, then you will mostly not need further encryption. You can identify a website's use of this protocol – hence: a website using encryption – by looking at the little "S" before the colon in your browser's address line (e.g. https://collaboration.cisv.org) or by the padlock symbol next to the URL in your browser.

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

You should tell anyone you send personal data to how important it is to keep it confidential and secure, and ask them to confirm they understand/agree.

Transfer of Personal Data Outside of the European Economic Area (EEA)

As a general rule, when you need to transfer personal data outside of the EEA, you must consider the following.

- Is adequate protection provided? (e.g. the information authorities have deemed a particular country or agreement safe)
- Are appropriate safeguards available? (e.g. importer offers "model clause contract")
- Whether an exception exists which permits the transfer, e.g. individual has consented to transfer, transfer necessary for the contract.
-

Within the CISV context, we are clear with people that we are an international organization and that we will share their information within CISV as needed in order to support their participation. We also emphasize the importance of confidentiality and security in many different ways.

Deleting or Destroying Personal Data

When it is no longer necessary to hold personal data, we must destroy it securely:

- You must shred paper or destroy it in a way that makes it impossible to read or use the data on it.
- You must delete electronic documents and clear the trash/recycle bin on your computer.
- Before you get rid of a computer or electronic storage device that has held personal data, you must consult experts to ensure that no data can be retrieved from it.
- Regularly ensure that you delete IRFs and other sensitive personal data from your email accounts when it is no longer necessary to store the information.

When to Report a Breach?

Across the European Economic Area (EEA) all breaches must be reported to the relevant local authority within 72 hours, unless the breaches are unlikely to result in risk to the person.

If you know or think there has been a breach of confidentiality, you should always talk with the person in your NA or Chapter who is responsible for data protection.

There are 3 basic things you should consider to help you to determine whether or not a breach has taken place and if it is serious:

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

- Was there a breach of security? – e.g. someone unauthorized got into the office – this may or may not mean that someone got access to personal data or that there is any risk to the individuals whose data is held there.
- Has someone who is not authorized got access to the data in some way? e.g. data is left on a train or someone hacks your system
- What are the possible risks to the rights and freedoms of the individual whose data was accessed? E.g. could their data be used for any purposes that they have not authorised, such as opening a credit account in their name?

Main Individual Rights to be Aware of

People have a right to know (this information is generally put in a Privacy Notice or is part of Terms and Conditions):

- Who we are as an organization
- If we have a Data Protection Officer, and who that is
- Why we are processing data and what is the good reason for us to do it
- Where the data came from if it came to us indirectly e.g. someone else gave it to us
- Who will receive the data
- Whether the data is being transferred outside the EEA and, if so, what safeguards are in place
- How long the data is kept and if we don't know just now, how we will we decide how long to keep it

People also have the right to:

- Withdraw consent to the use of their data (but there may be other very good reasons for using their data that means we can still use it, see above)
- Complain to the local/national supervisory authority or object to our use of their data
- Make a subject access request to see or have copies of any personal data held about them, generally free of charge – As an organizations we need to have the ability to search for and produce the personal data we hold, quite easily and quickly.
- Erasure – this is often referred to as the right to be forgotten – As an organization we need to be able to erase data. If we do not erase it, it is our duty to explain why we still need the data and should not erase it. Note that an organization may be obliged to erase data when it is relying on consent to use the data and consent has been withdrawn or when the individual has successfully objected to the relevant supervisory authority about failure to erase.

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

- Rectification – to have any incorrect data that is held about them made correct. This may be straightforward if it's factual data, but it can get complex when it's subjective data, like different versions of an incident. It may be that the best option is for us is to ensure that we keep both versions on our official record.

Fines

The GDPR will significantly increase the fines for breaches to a maximum of 20 million euros or 4% of annual worldwide turnover. Applies to organizations of all sizes.

QUESTIONS TO ASK OURSELVES

We can use this approach to assess risk before we start a new process to collect data or to assess existing processes.

- Describe the process
  - Is it necessary?
  - Is it proportionate, are we only asking for what we need?
  - By holding the data, do we create a risk for the individual? How much of a risk? If the risk is high, we have a greater responsibility to treat the data with care.
- What data have we got?
- What are we using it for?
- What is the justification or good reason (see above under 7 Principles) for using this data?
- Where is it stored?
- Who needs access to it?
- Who actually has access to it?
- Do people (which people) know what data we have, use and why?
- Is the data stored securely? Are there additional safeguards we can put in place?
- When (if ever) is the data no longer needed?
- When (if at all) is the data destroyed? How is it destroyed?

CISV International
Building global friendship

www.cisv.org
international@cisv.org
+44 (0)191 232 4998

MEA House, Ellison Place
Newcastle upon Tyne
NE1 8XS England

LINKS TO GUIDANCE

- General Data Protection Regulation (HTML/PDF options)
- The UK supervisory authority (ICO's) GDPR microsite
- The Article 29 working party's adopted guidelines
  - Data portability (wp242)
  - Data protection officers (wp243)
  - Lead supervisory authority (wp244)
  - DPIAs (wp248)
  - Breach notification (wp250)
  - Automated decision making and profiling (wp251)
  - Setting of fines (wp253)
- Awaited Article 29 working party guidelines (as at 19-Feb-18):
  - Consent (wp259)
  - Transparency (wp260)
  - Transfers on the basis of article 49(1) GDPR (wp262)
- European Commission guidelines "How to write clearly" (for privacy notices)
- Useful example of child-centred language in UN Convention on the Rights of the Child in Child Friendly Language
- ENISA has produced a methodology for assessing the severity of a breach