Data Protection Guidelines for Commission Members

Do's and Don'ts

Year of publication: 2020

About these guidelines

These guidelines establish a non-exclusive list of Do's and Don'ts that are intended to help Commission members in the course of fulfilling the Commissions' mandates established by the IUCN Statutes.

The purpose of these guidelines is to raise Commission members' awareness and understanding of both the applicability and the impact that data protection has on the work they undertake in their role as an IUCN Commission member. The aim is to ensure compliance.

How does data protection and privacy affect you as a Commission member?

As a network of experts, data protection and privacy applies to you when you use personal data in the course of IUCN work. In particular, in order to participate in IUCN work you agree that your information may be used and shared within the network and further you agree to respect other people's personal data that you may have access to. You also need to ensure that the systems you use when handling personal data are compliant. Non-compliance can have severe consequences for you and for IUCN and depending on the jurisdiction; violations can lead to substantial civil and criminal liability.

IUCN

Do's

1) **Do** familiarize yourself with IUCN rules and procedures including policies that concern compliance with data protection laws such as the IUCN Data Protection Policy (which is available at https://www.iucn.org/sites/dev/files/iucn_data_protection_policy.pdf) and with what it means to you and your work for IUCN.

2) **Do** support IUCN's commitment to protecting the security of personal data by handling any personal data provided to you in the context of IUCN work with due care and in accordance with the principles set forth in the IUCN Data Protection Policy and these Do's and Don'ts.

3) **Do** understand that compliance with data protection and privacy laws and regulations is not just about systems; it requires a change in behavior and how you work.

4) **Do** collect only the personal data you need.

The more information you collect the more responsibility you have towards the person you collect the personal data from. When you register participants for an event, think about the data collection fields you include on the registration form.

Example: do you really need to request a physical address if only an email address is needed for communication purposes?

Example: when running a survey in Survey Monkey, only ask for the information you need.

5) **Do** establish a legal basis for collecting personal data.

Personal data may be collected and used for the purposes of signing and implementing an agreement.

Example: an agreement signed by IUCN Secretariat on behalf of the Commission.

The data subject may have provided you with consent to use her/his personal data. Such consent needs to be documented.

Example: inviting participants to register for an event.

You may be required by applicable law or regulations to use or disclose certain personal data.

You may process personal data for a legitimate purpose pursued by IUCN

Example: In order to comply with an obligation imposed by IUCN Statutes.

6) **Do** ensure that personal data is kept confidential and limit access or sharing to those who need to know and are authorized to use it.

This means sharing personal data with only those who need it to do their work. This also means that personal data should not be shared on websites accessible to the public or other public online forums unless the data subject has expressly consented to such sharing.

What is Personal data?

Personal data is any information that relates to and enables a person ("data subject") to be identified such as a name, address, email address, an identification number, IP address, an online identifier, biometric data, cookies etc.

IUCN requires you to familiarize yourself with these guidelines and to comply with them.

7) **Do** use IUCN systems and tools available to you as they comply with the General Data Protection Regulation (GDPR).

We strongly recommend that personal data be stored in the global systems such as the IUCN Commission System, Union Portal and the Constituents Relationship Management (CRM). The advantage of using the global systems is that they are GDPR compliant. In addition, it enables IUCN Secretariat to handle any data subject access requests and to have the same process and standards applied to all the requests. If you manage your own mailing list outside of the global systems, the risk is that IUCN is not able to comply with some data subject requests linked to personal data stored outside the global systems. This creates liability for IUCN and could have potential financial as well as reputational consequences. It means also that you will have to handle data subject requests on your own and that IUCN will only be able to provide limited support to you. This could also create liability to you personally.

Example: Group leaders should insist or strongly encourage the members of their group(s) to keep their personal profile information up to date in the IUCN Commission System.

Example: Specialist Group leaders: do use the IUCN Commission System as your reference point, storage location for personal data of your group members. This is a secure, compliant system.

Do's

8) **Do** ensure that any newsletters you manage are GDPR compliant.

This means that you must have a legitimate basis to email the recipients of such newsletters based on consent or legitimate interest of IUCN. You must include a link to the IUCN privacy policy (see https://portals.iucn.org/dataprotection/privacypolicy) in your message and you must inform the recipients of their right to unsubscribe from the mailing list.

9) **Do** use BCC function when emailing a large group of people especially if they do not know each other.

Failure to use BCC means that you share names and addresses of recipients amongst the recipients without asking for their permission.

Don'ts

1) **Don't** disclose personal data to unauthorized persons.

This is because personal data is confidential information and should be protected from unauthorized access. Before sending any personal data, always check if the recipient needs to know this information in order to do his/her work.

2) **Don't** disclose personal data over the phone.

Divulging personal information over the phone (usually a person's name or email address) is not allowed. Verify the identity of the caller and the reason for the request so that you can propose a solution if appropriate.

Example: take a message.

3) **Don't** share CVs and other supporting documents by email.

Delete unsolicited CVs and advise applicants to apply through the relevant systems:

For applications to IUCN's Commission membership using the IUCN Commissions System at https://portals.iucn.org/commissions/

For applications to IUCN job positions via the Human Resources Management System (HRMS) at https://hrms.iucn.org/iresy/index.cfm?event=vac.showOpenList

For applications to consultancies in relation to IUCN's work, through the following links at: https://www.iucn.org/procurement https://www.iucn.org/regions/mediterranean/get-involved/work-us/consultancy-opportunities.

Don'ts

4) **Don't** keep personal data that is no longer needed in your personal devices (phone, computer).

This means deleting copies temporarily downloaded on local drives.

Example: by clearing the internet browser cache and/or deleting from the "Download" directory or equivalent.

6) **Don't** store personal data in excel files.

Personal data kept in an excel sheet is rarely updated and due to its decentralized nature is cumbersome to manage when data subjects ask not to receive communication from IUCN. This creates a risk for IUCN and could attract financial penalties as there is a chance that we would be sending communications to persons that have expressly asked not to receive such communication. For storage of personal data, refer to **Do** 7) above).

8) **Don't** make private or commercial use of personal data collected for IUCN work.

Example: Do not download IUCN mailing lists for personal and / or commercial use.

5) **Don't** store personal data in USB sticks, DVDs, external hard drive, cloud or social media platforms.

USB sticks, DVDs, and external hard drive can be misplaced or lost putting personal data stored in them at risk.

It is a common request to be asked if personal data may be exchanged in Google Docs. Google Docs is not considered a safe tool in regards to GDPR and therefore it is not recommended to be used within IUCN.

7) **Don't** leave paper and print outs of personal data accessible to unauthorized persons.

We recommend that you avoid printing any personal data. If you must print personal data, ensure that you destroy or shred it after use.

Example. Consult the CV of an applicant requesting to join a Commission or a Commission Specialist Group through IUCN Commissions System on the screen. If you need to print out this CV in order to better assess the application, destroy such CV as soon as this assessment is completed.

In case of doubt contact the Commissions Support Unit at *commissions@iucn.org*

IUCN, International Union for Conservation of Nature
Rue Mauverney 28
1196 Gland
Switzerland
Tel: +41 22 999 0000
Fax: +41 22 999 0002
www.iucn.org