UNIVERSITÉ DE GENÈVE

GENEVA CENTRE FOR PHILANTHROPY

unige.ch/philanthropy

DATA PROTECTION FOR NON-PROFIT ENTITIES

FONDATION HELENE&VICTOR BARBOUR

EDMOND DE ROTHSCHILD FOUNDATIONS

Fondation de France

FONDATION LEENAARDS

17 96 LOMBARD ODIER FONDATION

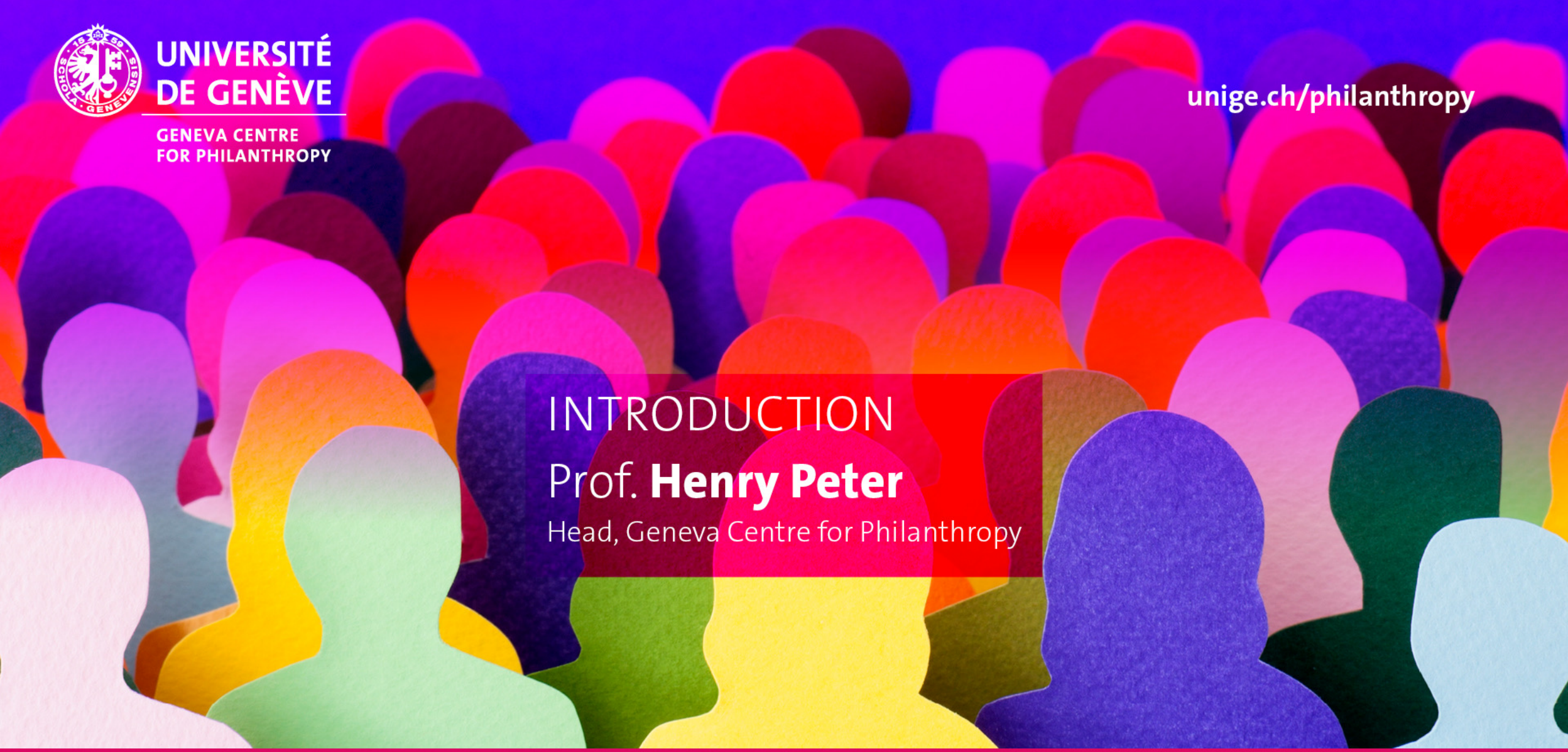
SwissLife Stiftung Perspektiven

UNIVERSITÉ DE GENÈVE

UNIVERSITÉ DE GENÈVE

GENEVA CENTRE FOR PHILANTHROPY

unige.ch/philanthropy



INTRODUCTION

Prof. **Henry Peter**

Head, Geneva Centre for Philanthropy

UNIVERSITÉ DE GENÈVE

GENEVA CENTRE FOR PHILANTHROPY

unige.ch/philanthropy

PANEL
MODERATED by

Vincent Pfammatter

Academic fellow of the GCP

Sebastian Rieger

Attorney-at-law, proFonds Legal Officer

Theodora Dragan

Data Protection Officer & Legal Counsel at CyberPeace Institute, Founding member of the Swiss DPO Association (ASDPO)

James de France

Senior Legal Counsel and Data Protection Officer at the International Federation of Red Cross and Red Crescent Societies (IFRC)

FONDATION HELENE & VICTOR BARBOUR

EDMOND DE ROTHSCHILD FOUNDATIONS

Fondation de France

FONDATION LEENAARDS

17 96 LOMBARD ODIER FONDATION

SwissLife Stiftung Perspektiven

UNIVERSITÉ DE GENÈVE

Dachverband gemeinnütziger Stiftungen der Schweiz

Switzerland's new data protection act: Important changes and the tried and tested

RA Sebastian Rieger, MLaw

DUFOUR Advokatur, Basel

proFonds, Dachverband gemeinnütziger Stiftungen der Schweiz, Basel

Overview

- Total revision of the Federal Act of Data Protection
- What has remained the same?
- Important changes
- Sanctions
- Summary

The new Federal Act of Data Protection (FADP)

- **Total revision of the FADP**
  - The FADP has been totally revised. The previous law dates from 1992.
  - The total revision was adopted by Parliament on 25 September 2020.
  - The new FADP is expected to enter into force in mid-2022.
  - This date is important because the law does not provide for any transition periods.

What has remained the same?

- **Purpose of the Data Protection Act: Protection of personality and constitutional rights**
  - Keywords: Personal freedom / privacy / informational autonomy
- **Accuracy of data**
  - The person responsible has to make sure that the data processed is correct. Incorrect data or false information must not be processed.
  - It is duty of the person responsible to ensure that the data is correct.
  - Incorrect or incomplete data must be corrected, deleted or destroyed.

What has remained the same?

- **Principles of data protection law**
  - Data processing must be legal / lawfull
    - The processing of personal data is permitted as long as it does not violate legal norms
    - In the EU, a different approach prevails: any data processing is initially illegal. Therefore, I must be able to justify any data processing (for example by a consent, contractual or legal obligations, overriding interest).
  - Data processing must be done in good faith.
    - Obligation to inform and notify in case of data protection violations can be derived
  - Data processing must be proportionate
    - This means processing only as much data as is necessary to achieve the purpose and no more. The creation of too large data collections is therefore not permitted (Privacy by design and by default: Art. 7 nFADP)
  - Data processing must have a recognizable purpose
    - Recognizable to the data subject
    - Processing compatible with this purpose

What has remained the same?

- **Technology-neutral approach: digital or analogue**
  - It does not matter whether the data processing is done digitally or with pen and paper.
- **Definition of processing:**
  - **Art. 3 lit. e FADP:**

  Any handling of personal data, **regardless of the means and procedures used**, in particular the acquisition, storage, use, reworking, disclosure, archiving or destruction of data.
  - **Art. 5 lit. d nFADP:**

  Any handling of personal data, **regardless of the means and procedures used**, in particular the acquisition, storage, retention, use, modification, disclosure, archiving, deletion or destruction of data.

What has remained the same?

- **Data security: appropriate technical and organizational measures (TOM)**
- **Examples**
- **Access control**: Access by authorized persons is limited to the personal data that they need to fulfil their task.
- **Entrance control**: Access to the facilities and installations where personal data is processed is denied to unauthorized persons.
- **Data carrier control**: Reading, copying, modifying, moving or removing data is made impossible for unauthorized persons.
- **Storage control**: Unauthorized entry into the data storage device as well as unauthorized inspection, modification or deletion of stored personal data is made impossible.
- **User control**: The use of automated data processing systems by unauthorized persons is prevented.

What has remained the same?

- **Order processing / processing by third parties**
  - Delegation by contract or law possible if
    - the data is processed in the same way as the data controller would be permitted to do; and
    - no legal or contractual obligation of secrecy prohibits the delegation
  - A delegation does not exclude the liability for person responsible

Important changes

- **Processing Register (Art. 12 nFADP)**
  - The processing register is used to record and check the individual data processing operations. Ultimately, it is a matter of tracing the processing operations.
  - Minimum content:
    - the identity of the person responsible
    - the purpose of the processing
    - a description of the categories of data subjects and the categories of personal data processed
    - Recipients
    - duration of processing, if possible
    - information on data security
    - Information if disclosure abroad

Important changes

- **Obligation to inform (Art. 19 ff. nFADP)**
  - Proactive information to data subjects
  - Purpose of the obligation to inform: Effective exercise of rights
  - Minimum information: Identity and contact of the data controller, purpose of processing, recipients and category of personal data, if applicable.
  - If the data is transferred abroad: country of destination, guarantees
  - If the data is not collected from the data subject: one month's notice.
  - GDPR goes much further
  - **Data protection declaration (information about data processing, the purpose, the data controller and the rights of the data subject)**
- **Data protection consequence assessment (Art. 22 f. nFADP)**
  - Prior examination of future data processing
  - High risk? Will data requiring special protection be processed on a large scale or will extensive public areas be systematically monitored?

Important changes

- **Notification of data security breaches (Art. 24 nFADP)**
  - Notification of a data security breach
  - Notification to the Federal Data Protection and Information Commissioner (préposé fédéral à la protection des données et à la transparence [PFPDT]) if there is a high risk to personality or fundamental rights
  - Notification to data subject if necessary for protection or if required by the FDPIC
  - Deadline: as soon as possible
- **Right to receive information (Art. 25 nFADP)**
  - Information on the scope of processing, purpose of processing and duration of processing
  - Information about the person responsible, the processor and the recipient
  - Information about contact options
  - Possibilities of removal and deletion

Sanctions according to the nFADP (Art. 60 ff.)

- **Subsidiary criminal law (Nebenstrafrecht)**
  - Violation of obligations to inform, provide information and cooperate
  - Violation of obligations of care (disclosure abroad, unauthorized processing of orders, failure to comply with minimum data security requirements)
  - Violation of professional secrecy
  - Failure to comply with orders of the Federal Data Protection and Information Commissioner
  - Only intentional violations
  - Responsible: Responsibility of the cantons, usually the public prosecutor's office.
- **Personal liability**
  - Personal liability means that the natural person is liable, e.g. the employee, in the EU it is the company that is liable
- **Very high penalties**
  - Deterrence (Abschreckung) with penalties of up to CHF 250,000

Summary

- **Far-reaching requirements for the person responsible**
  - Technical and organizational measures (TOM)
  - Implementation costs
  - Personnel costs: Sensitization of the employees
  - Restructuring
- **Data protection is part of the risk management**
  - Identify the risk (processing as risk)
  - Assessment and risk evaluation (Data protection consequence assessment)
  - Risk management or risk minimisation by using TOM
  - Controlling the effectiveness of the TOM

Thank you for your attention!

proFonds
Sebastian Rieger, Advokat
Dufourstrasse 49
4010 Basel
Tel. 061 205 03 03
Fax 061 205 03 04
www.dufour-advokatur.ch
sebastian.rieger@dufo.ch

CyberPeace Institute

CyberPeace Institute

A Swiss foundation supporting beneficiaries worldwide

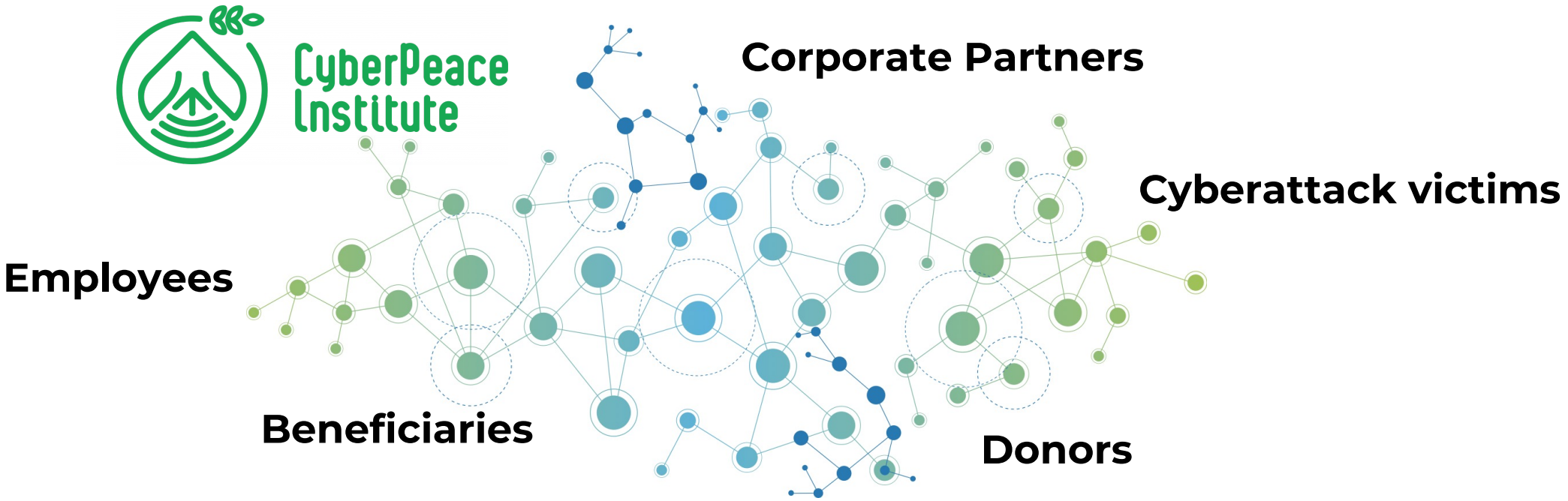
Who we are

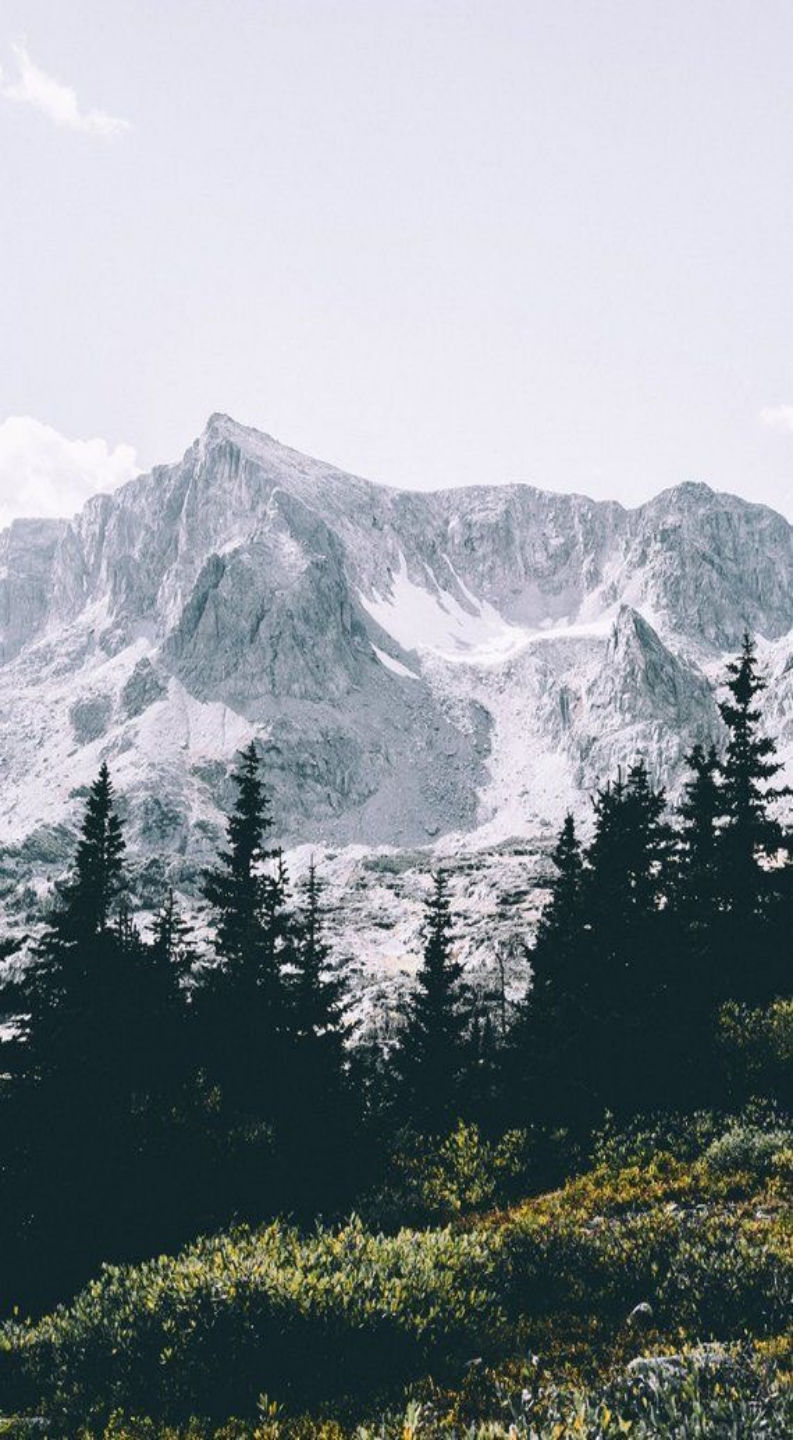
- Independent NGO, launched 2019
  - escalating dangers of cyberattacks
- Founded by Corporate entities and Foundations
- Funded
  - Core support, project based funding
  - Corporates & Philanthropy
- HQ in Geneva

No one is safe in cyberspace until we all are.

Context

- Increasing digitalization for work, trade, entertainment, critical infrastructure
- People-centric focus: cyberspace is about people, not technology





Main challenges

1. Ensuring lawful data collection
    - Legal basis
    - Documentation
2. Respecting data transfer rules
    - Know your transfers
    - Standard Contractual Clauses (OK for Switzerland)
    - Limitations of consent
3. Implementing data protection across the lifecycle
    - Evaluate service providers
    - Access limitation, access control
    - Back-ups and Plan B
4. Preventing human error

… and solutions

1. Data minimisation
2. Privacy by design
3. Privacy by default
4. Frequent training
5. Get everyone on-board
6. Good processes
7. Reliable service providers

To conclude...

The heart of the CyberPeace Institute's mission:
to achieve a cyberspace at peace, for everyone, everywhere

No one is safe in cyberspace, until we all are.

Thank you

info@cyberpeaceinstitute.org

https://cyberpeaceinstitute.org

@CyberpeaceInst

@CyberpeaceInstitute

@CyberpeaceInst

@CyberPeace Institute

International Federation
of Red Cross and Red Crescent Societies

Data Protection at IFRC

The Geneva Centre for Philanthropy

November 16, 2021

James De France, IFRC Senior Legal Counsel - DPO

Status of IFRC

- IFRC is an International Organization
  - Status/HQ agreements with 91 countries granting IO status along with privileges and immunities. Also recognized as an IO by EU, US, UN
  - Subject to its own legal framework: Financial regulations, Staff Rules, Codes of Conduct, Data Protection Policy - based on recognized principles and best-practices
  - Maintain independence, facilitate consistent practices across offices, legal certainty

- IFRC is the secretariat providing support to 192 National Societies
  - Each subject to the national law of its host country
  - Created under different legal structures, considered as NGOs
  - Collectively, the world's largest humanitarian network – hundreds of thousands of staff, millions of volunteers – reaching over 100 million people each year

Data Protection Concerns

- We collect and process huge amounts of personal data, including sensitive data, from vulnerable individuals, and in very challenging contexts.
  - How can we choose the right legal bases, minimize data collection to what is necessary, explain our data processing activities to those we serve, and ensure protection of the data throughout its lifecycle?
- How can we balance our IO status against partners'/contractors' obligations to comply with data protection laws?
- Can we balance the neutral provision of services against the demands of donors and counter-terrorism measures and sanctions regimes?
- Can we maintain a strong level of data protection as more processes are digital, cloud-based and our activities involve a growing number of partners?

Our approach

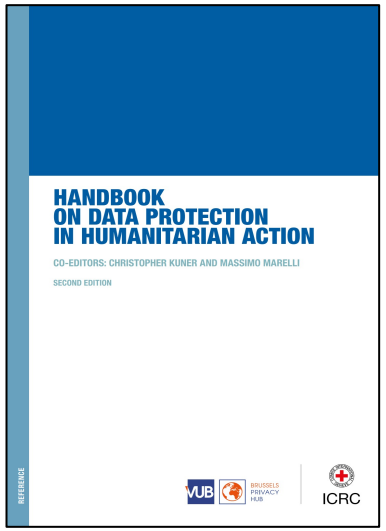
- Develop a policy in consultation with all departments
- Face-to-face training sessions
- DPO involvement in the development of data collection projects and tools
- DPO involvement in contract negotiations
- Developing practical guidelines – Cash, IM
- Developing Training Modules and Templates – Data Sharing
- Convening experts from various sectors into a DPSC
- Undertaking DPIAs for higher-risk data processing (health-related, biometrics)
- Data breach reporting and data classification tools
- Keeping an “open door”

Engagements with Partners

- Part of a diverse group of NGO, corporations, IOs and academia contributing to the second edition of the Handbook for Data Protection in Humanitarian Action
- Participation in EU working groups aiming to address the data protection issues specific to international organizations – focus on data transfers
- Presenting on data protection matters for IOs and a new Humanitarian DPO certification course through Maastricht University
- Development of data protection online course materials together with Data Literacy
- Joint publications with IOM, UN OCHA, ICRC and other RCRC NSs helping to make data protection best-practices practical for the wider humanitarian community.

THANK YOU

Resources



- Mémento RGPD - France générosités - réédition 2020 : Calaméo - Mémento RGPD - France générosités - réédition 2020 (calameo.com)
- ICRC Handbook on Data Protection in the Humanitarian Sector, downloadable here : https://www.icrc.org/en/data-protection-humanitarian-action-handbook
- Article on Data Protection in the non-profit sector, downloadable here https://www.unige.ch/philanthropie/files/9115/5292/2491/Data_Protection_and_the_Swiss_Non-Profit_Sector.pdf
- Fundraising and data protection: https://ico.org.uk/for-organisations/fundraising-and-data-protection/
- Guide de sensibilisation au RGPD pour les associations: https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide_association.pdf

EVALUATION

Thank you for taking a few minutes to complete the evaluation questionnaire:

https://unige.ch/-/pldata

UNIVERSITÉ DE GENÈVE

GENEVA CENTRE FOR PHILANTHROPY

unige.ch/philanthropy

UPDATE ON THE GCP'S ACTIVITIES

Laetitia Gill

Executive Director, Geneva Centre for Philanthropy

TEACHING

Academic course – Autumn 2021

- **The Many Faces of Philanthropy (A & B)**, Faculty of GSEM, Prof. Ugazio & Dr Monks
- ***L'éthique de la philanthropie***, Faculty of Humanities (department of Philosophy), Dr Tieffenbach

Continuous education programme

- DAS in strategic (CAS 1) and operational (CAS 2) philanthropy, Faculty of GSEM (Sept. 2021-August 2022)

NEXT EVENTS

- **02.12.2021** Building bridges, Geneva, **"Financing sustainable initiatives and social entreprises: innovative means**" (Sustainable Finance Geneva)

- **06.12.2021** Philanthropy Lunch ***"D'une action de terrain à un modèle reproductible***"

Panel with Dr. Rochat, Dresse Benski and Prof. Benagiano, moderated by Prof. Geissbuhler

- **01.02.2022** *Rencontre Maison Internationale des Associations*, Geneva, ***"Activité économique et fiscalité"***

- **08-09.06.2022 –** International Conference on **Social entrepreneurship**, Geneva. In collaboration with the Schwab Foundation

UNIVERSITÉ DE GENÈVE

GENEVA CENTRE FOR PHILANTHROPY

unige.ch/philanthropy

CONTACT

Centre en Philanthropie
Uni Dufour
24, rue du Général-Dufour
CH-1204 Geneva

W: **www.unige.ch/philanthropie**

T: + 41 22 379 76 18

Follow us on LinkedIn