

Workshop on Data Protection in International Organizations

Co-hosted by the European Data Protection Supervisor
and the UN World Food Programme



12 – 13 May 2022



WELCOMING REMARKS

[Redacted]

[Redacted]

, WFP





WELCOME & KEYNOTE

Wojciech Wiewiorowski
European Data Protection Supervisor





KEYNOTE

[REDACTED]
[REDACTED] Eticas Consulting

Trends in Privacy & Data Protection in International Organizations



- [REDACTED] Italian Data Protection Authority [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED], ICRC
- [REDACTED], UNESCO

Moderator: [REDACTED] Information & Communication Officer, EDPS



[REDACTED]

[REDACTED]



**Working Group on the Role of Personal
Data Protection in International
Development Aid, International
Humanitarian Aid and Crisis
Management (WG AID)**

**Workshop : Data Protection within International
Organizations**

Organized by the EDPS and the WFP
Rome, 12 May 2022





Origin of the WG AID



- The GPA resolved to contribute, at its level, to the achievement of the UN's Agenda 2030, by identifying and engaging relevant stakeholders in international development aid in order to achieve its longer-term strategic goal of a **global regulatory environment with high, clear and consistent standards of data protection.**
- October 2020: To this end, the 42nd GPA adopted a Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis, which set up the WG AID.



Contributing Authorities



1. **Association francophone des Autorités de protection des données personnelles (AFAPDP)**
2. **Commission de l'Informatique et des libertés (CIL), Burkina Faso**
3. **Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe**
4. **Data Protection Commissioner of the CoE, Council of Europe**
5. **European Data Protection Supervisor (EDPS)**
6. **Commission Nationale pour la Protection des Données à Caractère Personnel, (CNPDCP), Gabon**
7. **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Germany**
8. **International Committee of the Red Cross (ICRC)**
9. **International Organization for Migration (IOM)**
10. **Office of the Information Commissioner (JOIC), Jersey**
11. **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Mexico**
12. **Commission de contrôle des informations nominatives (CCIN) – Co-chair, Principauté de Monaco**
13. **Comissão Nacional de Protecção de Dados (CNPD), Portugal**
14. **Commission de Protection des Données Personnelles (CDP), Senegal**
15. **Federal Data Protection and Information Commissioner (FDPIC) – Chair, Switzerland**
16. **Office of the Privacy Commissioner (OPC) , New Zealand**
17. **Information Commissioner's Office (ICO), UK**
18. **United Nations High Commissioner for Refugees (UNHCR)**



Objectives of the WG AID



1. to respond to the **request for cooperation** from relevant parties to develop guidelines and **share best practices in privacy and data protection** relating to international development assistance and international humanitarian action;
2. to develop an **advocacy and engagement strategy** with relevant stakeholders.



Highlights of 2021



1. **Geographical and Thematic Mapping of Relevant Actors**

- Complex
- Wide range of topics
- Importance of digital technology
- 72 countries that do not yet have a data protection legislation

2. **Elaboration of a questionnaire** on the data protection practices of the relevant actors



Agenda for 2022-23 (I)



- **Sending of the questionnaire** to over 70 actors (February);
- **Analysing the questionnaire responses** : identification of the pressing issues, promotion of the work of the GPA, possible revision of the WG's work plan;
- If needed, **interviewing key players** such as the UN special rapporteur on the right to privacy;
- Organizing **a workshop/webinar** bringing together the data protection community and development actors to discuss data protection issues and promote data protection;



Agenda for 2022-23 (II)



- **Producing guidelines** for the operators in charge of the execution of the programmes;
- **Maintaining and exploring possible synergies** with others WG and external stakeholders, such as:
 - The DigitHarium
 - The Humanitarian Data and Trust Initiative
 - The International Organisation of la Francophonie;
- **Pursuing the work** initiated in 2015 with the **ICRC** by cooperating on the 3rd Edition of the handbook and participating in the [Data Protection Officer in Humanitarian Action certification course with the University of Maastricht.](#)



**For more information or to
contact the WG AID**



- **Global Privacy Assembly Website:**
<http://globalprivacyassembly.org>





ICRC



TRENDS IN PRIVACY & DATA PROTECTION IN INTERNATIONAL ORGANIZATIONS

[REDACTED]

[REDACTED]

[REDACTED]



KEY DEVELOPMENTS

- Handbook 3rd Ed.
- R&D – A Delegation for Cyberspace
- Humanitarian Action Programme
- ICRC – UNHCR DP Framework Agreement
- WG Global Privacy Assembly



R&D - A DELEGATION FOR CYBERSPACE

- Testing Ground for R&D
 - Cooperation with EPFL & ETHZ
- Operating in a digital environment
- Cooperation with Luxembourg

EPFL

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



HUMANITARIAN ACTION PROGRAMME

- DPO in Humanitarian Action Training and Certification Programme
 - 2021: Geneva, Mexico*, Dakar
 - 2022: Nairobi, Bangkok, Amman, Geneva
 - Approx 150 ppl trained so far
- Alumni / Community of Practice
- Research
- Special Issue: Maastricht European and Comparative Law Journal
- And more!



ICRC – UNHCR DP FRAMEWORK AGREEMENT

- A Framework Agreement
- DP at the centre
- Enabler of cooperation
- Structure

18:00 4G

← Tweet

 UNHCR, the UN Refugee Agency
@Refugees

Now, more than ever, UNHCR is committed to protecting the personal data of people forced to flee.

Today @FilippoGrandi and @PMaurerICRC signed a Memo of Understanding between UNHCR and @ICRC to better coordinate on use and confidentiality of personal data in humanitarian action.



Tweet your reply

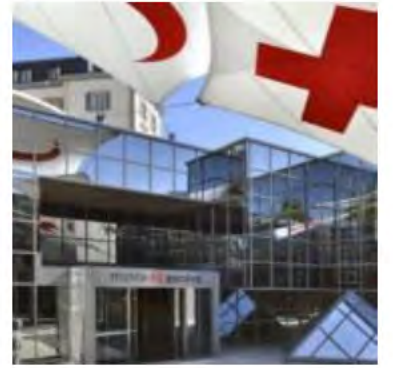
     



WG GLOBAL PRIVACY ASSEMBLY

- The GPA, Members and Observers
- Background: the Resolutions
- WG and its work
- Turkey 2022





Thank you!





UNESCO

UNESCO'S PRINCIPLES (1):

- In July 2021, the UNESCO Secretariat approved its first *Principles on Personal Data Protection and Privacy*.
- First time UNESCO has a dedicated corporate policy on data privacy.



UNESCO'S PRINCIPLES (2):

- UNESCO's Principles are based on the *Principles on the Protection of Personal Data and Privacy for the UN System Organizations*, endorsed by UNESCO, and formally adopted by the UN's High Level Committee on Management at its 36th Meeting in 2018.
- UNESCO's *Principles* form the core of an organizational policy framework that includes an implementation roadmap; a guideline; a privacy breach procedure; a portal hosting supporting guidance notes and templates, including a privacy impact assessment; a privacy KPIs dashboard; virtual and in-person training offerings; and, logs of business support requests, data subject requests (DSARs), and personal data incidents.



KEY DEVELOPMENTS (1):

- Drafting and adoption of the Principles via a cross-functional working group and internal policy approval mechanism
- House-wide senior management level communication.
- Inclusion in a memorandum to Members States on UNESCO's *New high-impact tools, policies and practises.*
- Establishment of the DPO role in the Executive Office of the Administration and Management Sector



KEY DEVELOPMENTS (2):

- Embedding contractual clauses and privacy notices, inc. a new website notice
- Training and awareness sessions, including multi-day sessions in UNESCO Category 1 Institutes
- Strong working relationships developed with the UNESCO Legal Office, with Partnerships, Procurement, Risk Management, and recently, with key members of the new IT management team.



BIGGEST CHALLENGES :

- Bridging corporate and programmatic work on privacy
- Building and sustaining an effective privacy training programme
- Pushing and pulling the privacy awareness programme, including how to introduce mandatory training in an Organization already fatigued by mandatory trainings.
- Institutionalization of **privacy impact assessments** and **due diligence** at UNESCO Headquarters, its 50 or so Field Offices, and its 9 Category 1 Institutes
- Measuring, monitoring and reporting effectively at appropriate level(s)
- EU Pillar 9 Assessment follow-up
- Personally, staying current and informed in a rapidly evolving field of knowledge



ON THE PROGRAMMATIC SIDE (1):

- On 23 November 2021, 193 Member States adopted by acclamation the *Recommendation on the Ethics of Artificial Intelligence*.
- This voice of global consensus calls on UNESCO's members to ensure more inclusive, diverse and fair outcomes when using these game-changing technologies.
- To ensure the full enactment of the rule of law, the Recommendation asks member countries to enact strong enforcement mechanisms and remedial actions to make certain that human rights and fundamental freedoms are respected in the digital world as they are in the physical world.
- It also calls for members to improve their capacities to deal with these technologies.



ON THE PROGRAMMATIC SIDE (2):

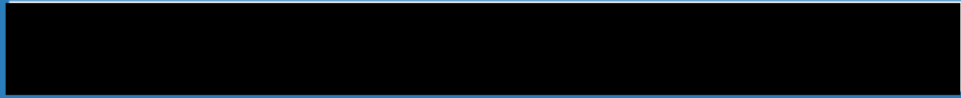
- The Recommendation is based on interconnected values and principles.
- The principles include familiar concepts of proportionality, security, transparency and accountability, but also explicitly include the 'right to privacy and data protection'.
- The Recommendation states that:
 - Privacy must be respected, protected and promoted throughout the lifecycle of AI systems;
 - Adequate data protection frameworks and governance mechanisms should be established in a multi-stakeholder approach at the national and international level, protected by judicial systems, and ensured throughout the lifecycle of AI systems; and,
 - Algorithmic systems require adequate privacy impact assessments, which include societal and ethical considerations of their use and an innovative use of the privacy by design approach.



Data Subjects' Rights: Challenges & Opportunities in IOs

- [REDACTED] Italian Data Protection Authority
- [REDACTED] European Space Agency
- [REDACTED] UNICEF
- [REDACTED]

Moderator: [REDACTED] OECD



ESA

Data subjects rights: challenges and opportunities in international organisations

02/05/2022

Overview

Data subject rights: EU and IGO context

European Space Agency (ESA) Protection of Personal Data Context and Policy

ESA Protection of Personal Data Policy and Data Subject Rights

Implementation of Data Subject Rights

European Organisations, e.g.

- The right of access of data subjects is enshrined in **Art. 8 of the EU Charter of Fundamental Rights**
- **Art. 15 GDPR**: Right of access by the data subject
- **EC 2018/1725: Art. 14; 48, 59; 65**

International Organisations, e.g.

- **CoE, Article 9**: Rights of the data subject
- **ESA PDP Article 5.4**: Data Subject's Rights



Context

- Protection of Personal Data Framework
- Independent Supervisory Authority
- Data Protection Committee
- DPO

ESA Personal Data Protection Framework

The European Space Agency is subject to a Personal Data Protection framework composed of the following elements:

1. The Principles of Personal Data Protection, as adopted by ESA Council Resolution (ESA/C/CCLXVIII/Res.2 (Final)) adopted on 13 June 2017
2. The Rules of Procedure for the Data Protection Supervisory Authority, as adopted by ESA Council Resolution (ESA/C/CCLXVIII/Res.2 (Final)) adopted on 13 June 2017
3. The Policy on Personal Data Protection adopted by Director General of ESA on 5 February 2018 and effective on 1 March 2018

ESA Framework on Personal Data Protection:

- http://www.esa.int/About_Us/Law_at_ESA/Highlights_of_ESA_rules_and_regulations

About ESA Data Subject Rights: enable the validation of the lawfulness and the accuracy of the processed data by facilitating the exercise of rights

5.4 Data Subject's rights

5.4.1 The following rights of the Data Subjects, regardless of whether Personal Data have been obtained from the Data Subject, shall be recognised and protected by the Agency:

i. **The right to be informed, in a transparent manner**, as reasonably practicable, about:

(a) the identity of the Data Controller and the contact details of the Data Protection Officer;

(b) the purpose of the Data Processing, in case his/her Personal Data are Processed;

(c) the Data Recipients to whom his/her Personal Data shall be Disclosed;

(d) the existence of the rights mentioned in this Section 5.4.1 paragraphs ii., iii. and iv. below;

(e) **the time-limits for storing the Personal Data** (or the criteria used to determine the time-limits) as decided, in compliance with Section 5.2, by the Director General upon proposal of the Data Protection Officer (following consultation of the Department in charge of personnel matters, the Record Manager and other relevant Departments); and,

(f) **the practical modalities of exercising the rights** set forth in this Section 5.4.1 paragraphs ii., iii. and iv.

The right for every Data Subject to make a reasonable request for access to the Personal Data relating to him/her; in addition, in the case of Health-related Sensitive Personal Data, the conditions under which access is granted are those corresponding to generally applicable medical professional standards, as recommended by the Agency's medical advisor;

iii. **The right for every Data Subject to have his/her Personal Data erased, rectified, completed, or amended** as per the conditions set under Section 5.1. i. of this Policy;

iv. **The right for every interested Data Subject to lodge a complaint** before the Supervisory Authority in case the former demonstrates or has serious reasons to believe that a Data Protection Incident occurred in relation with his/her Personal Data, following a decision of the Agency (e. g. Data Protection Officer). Such complaint shall be lodged in accordance with the Rules of Procedure of the Supervisory Authority.

5.4.2 The right of information under Section 5.4.1 i. and the right of access under Section 5.4.1 ii. shall not apply:

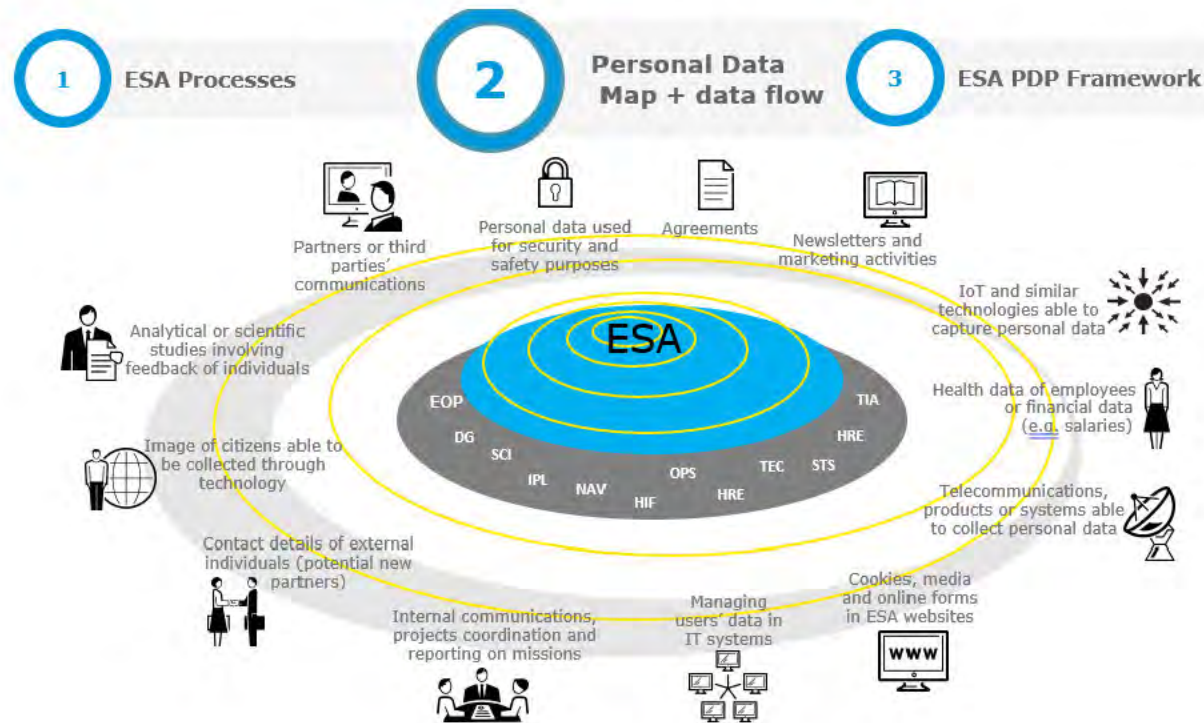
(a) where and insofar as the Data Subject is already in possession of the information;

(b) for the right of information, when processing of Personal Data is necessary for any Investigation or Dispute Resolution Procedure;

(c) for the right of access, where and insofar such access would conflict with an Investigation Procedure concerning the Data Subject.

- Policy Implementation:
 - **Data map:** processes and mapping of personal data – aligned with ADMIN ORG, QMS
 - **Notification records:** DPNR:
 - Privacy by Design, Privacy by Default, IT Tool Catalogue
 - Retention
 - Risk Assessment, mitigation: DPIA, TIA, Technical Annex
 - Procurement: Legal Agreements, Legal Arrangements, NDA/NDU, PDP Annex, ESA SCCs, Administrative Agreement, etc.
 - Procedures, Implementing instructions, Data Protection QMS processes
 - **Data Subject Rights**
 - Protection: Security: IT Security, Security classification, Project System Security
 - Accountability
 - Data Quality/ Accuracy
 - legitimate purpose,
 - Incident mgmt., etc.

Which personal data is held where for how long?



- Ca. 900 processes in the data map
- Documents the personal data flow throughout the data lifecycle
- Impact on protection, IT tools configuration, procurement contracts, etc. and:

Data subject rights, e.g.

- Where is the personal data held
- For how long
- Source of the personal data



Implementation the request

Within 30 days



Inform the Data Subject about the processing (e.g. privacy notice)
Note the date of the request (+ 30 days)

Is personal data involved? Does it involve personal data about others?
Request identification, authorization

Assess the scope: which personal data of the individual, time period, pseudonymised data, etc. May request further scope clarification

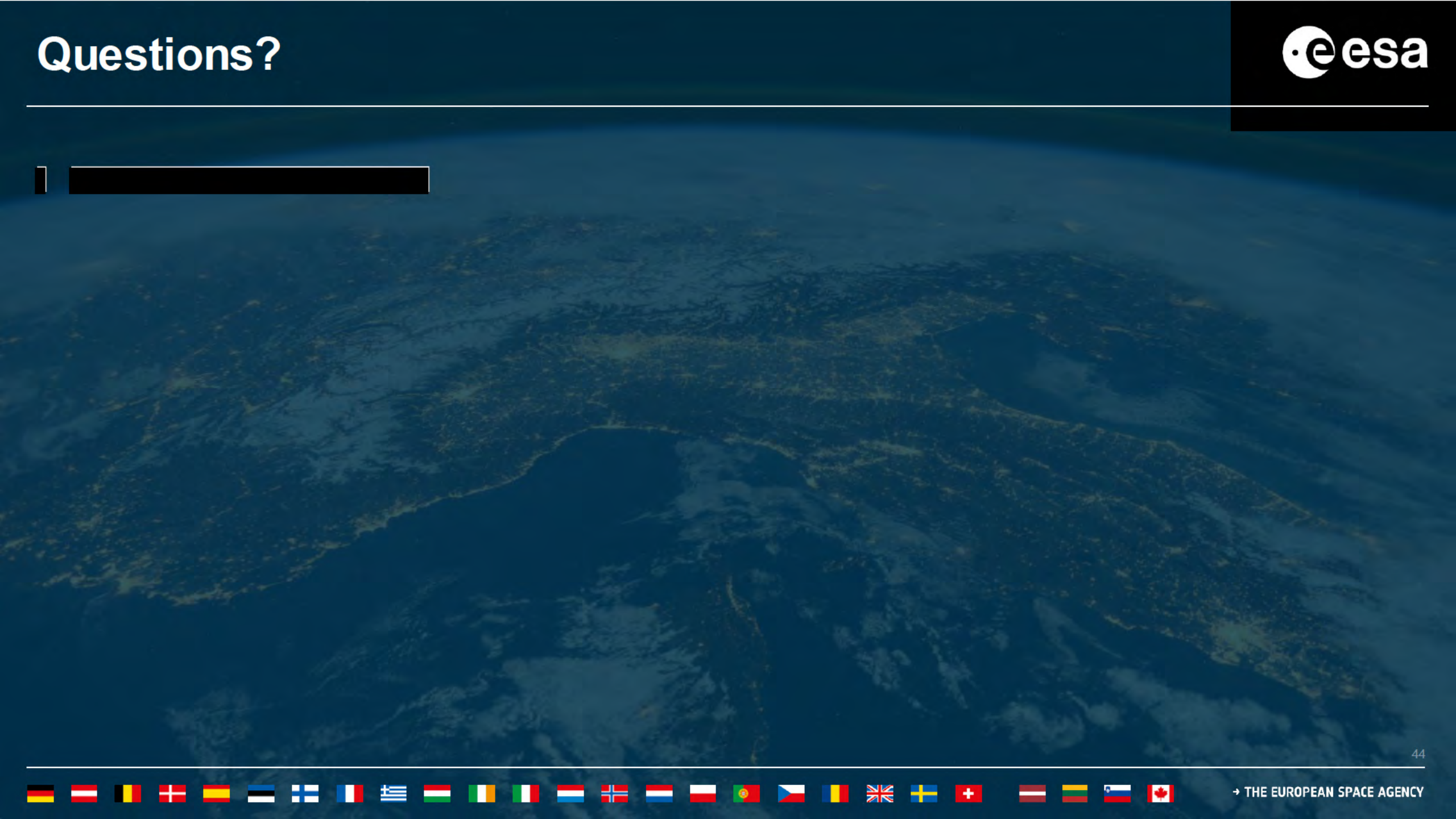
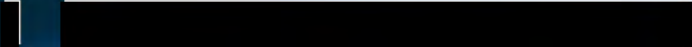
Respond to the request: which personal data is held, provide access and provide required information on the legitimate purpose, time period of processing, etc. while providing protection

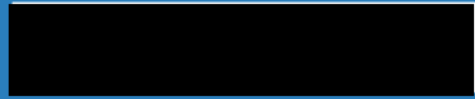
Identify the personal data

Check limitations

Provide access: easily accessible, transparent, e.g. provide a copy

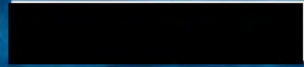
Questions?





UNICEF

Data Protection: Data Subject Requests



UNICEF Policy on Personal Data Protection

- Implementation is responsibility of each Division
- **All** personal data (of living individuals) processed/collected by UNICEF
 - Beneficiaries
 - Staff (and candidates)
 - Vendors
 - Donors
- *“UNICEF personnel shall take particular care in processing the personal data of children and vulnerable categories of data subjects.”*

Elements of the Policy

- Legitimate and fair basis for processing
 - i. **Consent** of the data subject, or the child's representative where appropriate;
 - ii. Contract
 - iii. Vital interests
 - iv. UNICEF / Beneficiary Interest
 - v. Legal obligation
 - vi. other legitimate interests of UNICEF consistent with its mandate, including the establishment, exercise or defense of legal claims or for UNICEF accountability
- In Emergency context, the Emergency Director may (upon consultation) derogate elements of the Policy

Data Subject Requests

- Data Subjects requests:
 - Access
 - Correct
 - Delete
 - Object to and restrict processing
 - Restricted automated decision-making
- Aligned with the UN Personal Data Protection And Privacy Principles
- Data subject requests can be done by the child* or their representative*
 - Assessment or response to the request shall consider the best interest of the child

Enabling Data Subject requests

- Ensure balance between data subject rights and handling requests
 - Consent / Purpose / Actual Use
- De-centralized & Diverse
 - Implementation of Policy devolved to the implementing parties
- Project/Platform specific: “By design and by default”
 - Reflected in software development requirements, operational SOPs, and others.

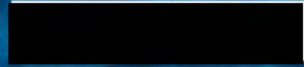
Examples

- Case 1: Informing data subjects of their rights through **privacy notices** and **consent forms**, e.g. unicef.org
- Case 2: Data Subject can contact the service via **dedicated e-mail** e.g. cash transfers
- Case 3: Good **data inventory** management **system** and good assignment of **roles** e.g. Information Sharing Protocols
- Case 4: **Contacting** the user at their registered e-mail, e.g. Voices of Youth
- Case 5: Analyzing & **Addressing**, e.g. through data inventory management and tech capability - e.g. Agora.unicef.org

Challenges & Opportunities

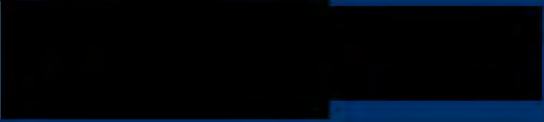
- Diverse types of engagements
- Decentralized system
- No central overview
- Possibility to establish review mechanism of the response or request
- Possibility to establish structured process

Data Protection: Data Subject Requests

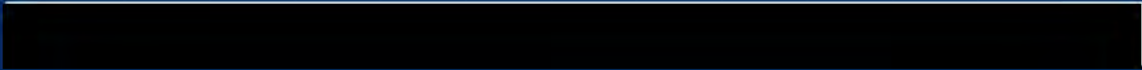


[REDACTED]

[REDACTED]



Data Subjects' Rights: challenges and opportunities in International Organizations:



May 2022



Index


- 01 Managing data subject's rights
- 02 Challenges and opportunities
- 03 Type, volume & tipology
- 04 Curiosities

- Practical
- Technical
- Governance
- Regulatory

01 Managing data subject's rights



Practical perspective (I)

- Before GDPR, Directive 95/46 was quite open, so each country decided via local Law the way to answer, content, deadlines, etc. So 27 very different ways to answer subjects rights for a Company in Europe.
- GDPR stated common obligations and one deadline for all rights (one month). 
- ██████ already had a protocol for the so called ARCO rights, (bow in English) with two places: one for employees (internal) and another for clients & others.
- DPO developed *in house* new protocols and procedures for old and new rights, with an extended team, new models, documents, Q&A's, and provided training to the team.

01 Managing data subject's rights



Practical perspective (II)

- For employees we did the same works, keeping the internal way to exercise the rights.
- We also made new protocols for other data subjects, such as shareholders, providers, signatories of contracts who represent companies, etc. setting up new addressess.

01 Managing data subject's rights



Technical perspective

- Focused on client rights: there are lots of data bases where personal information is under processing, being managed by different teams. The complexity *to open a window* (architects dixit) to all of them for the team who is in charge of GDPR's rights is huge.
- There is a team fully dedicated to manage them. They receive requests through mail, email and post office box. The answer should be given using the same way chosen by the client.
- There is also another way: an internal tool for branches and *client's personal managers*: BBVA's employee upload client's requests made before them, and GDPR's rights team receive and handle them.
- Right to data portability: fully automatized, in 24 hours the data subject receive the info.

01 Managing data subject's rights



Governance and regulatory perspective

- Over the years our governance has been refined, and the team know they can contact me directly when there are issues they do not know how to handle.
- Regarding regulatory perspective, the attention to these rights used to be an *in house* norm, however this year we transform the norm into an internal procedure.

02 Challenges and opportunities

Challenges (I) 🙄

- Sometimes understanding what the data subject is asking is a real challenge!
- To keep data under control so the *windows* for the GDPR's rights team work (able to access all personal data); considering *open new windows* in other or new databases.
- To keep information in documents, protocols, internal timelines & procedures updated. (e.g. recent issue with the ID in Spain).
- Avoiding other data subjects using client addresses to exercise GDPR's rights, as the answer may be zero data. This requires sometimes asking the data subject and readress their requests internally.

02 Challenges and opportunities

Opportunities (II) 😊

- ▲ It is a way to foresee potential reports to the Data Protection Authority early.
- ▲ It helps to see and fix internal mistakes e.g. clients receiving marketing when they should be labelled as *Robinson*.



03 Type, volume & tipology

Statistics (I)

2018	ACCESS	RECTIFICATION	CANCELLING	OBJECT	BLACKLIST FILE ERASURE	PORTABILITY
JANUARY	17	12	36	135	46	0
FEBRUARY	20	21	178	643	46	0
MARCH	23	17	108	616	49	0
APRIL	16	14	58	340	49	0
MAY	23	24	155	529	51	0
JUNE	17	22	176	323	47	2
JULY	18	24	96	229	125	0
AUGUST	14	33	80	120	77	1
SEPTEMBER	14	25	97	166	99	0
OCTOBER	16	34	150	211	113	0
NOVEMBER	18	33	120	203	82	0
DECEMBER	8	23	105	216	54	0
TOTAL	204	282	1359	3731	838	3

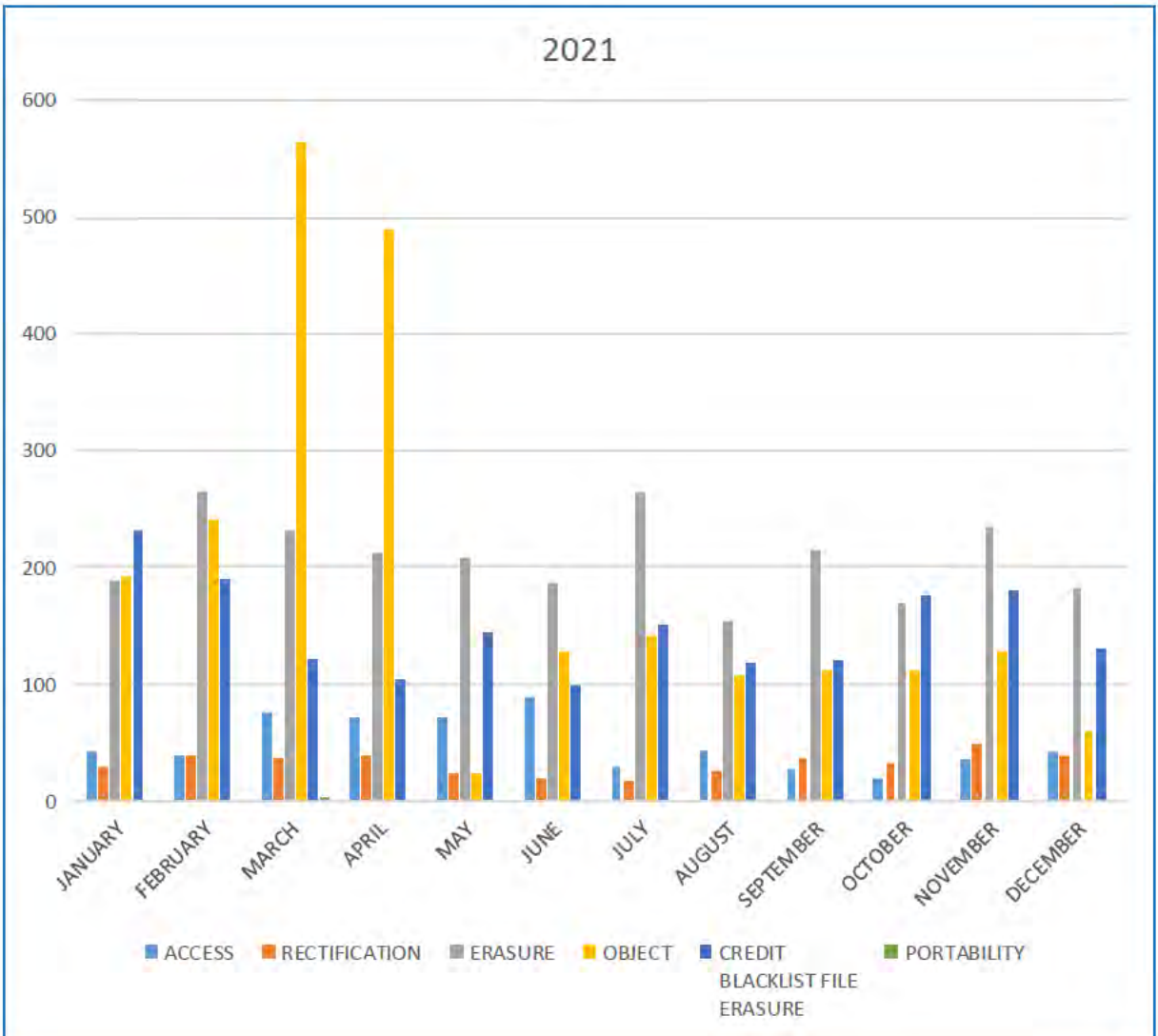
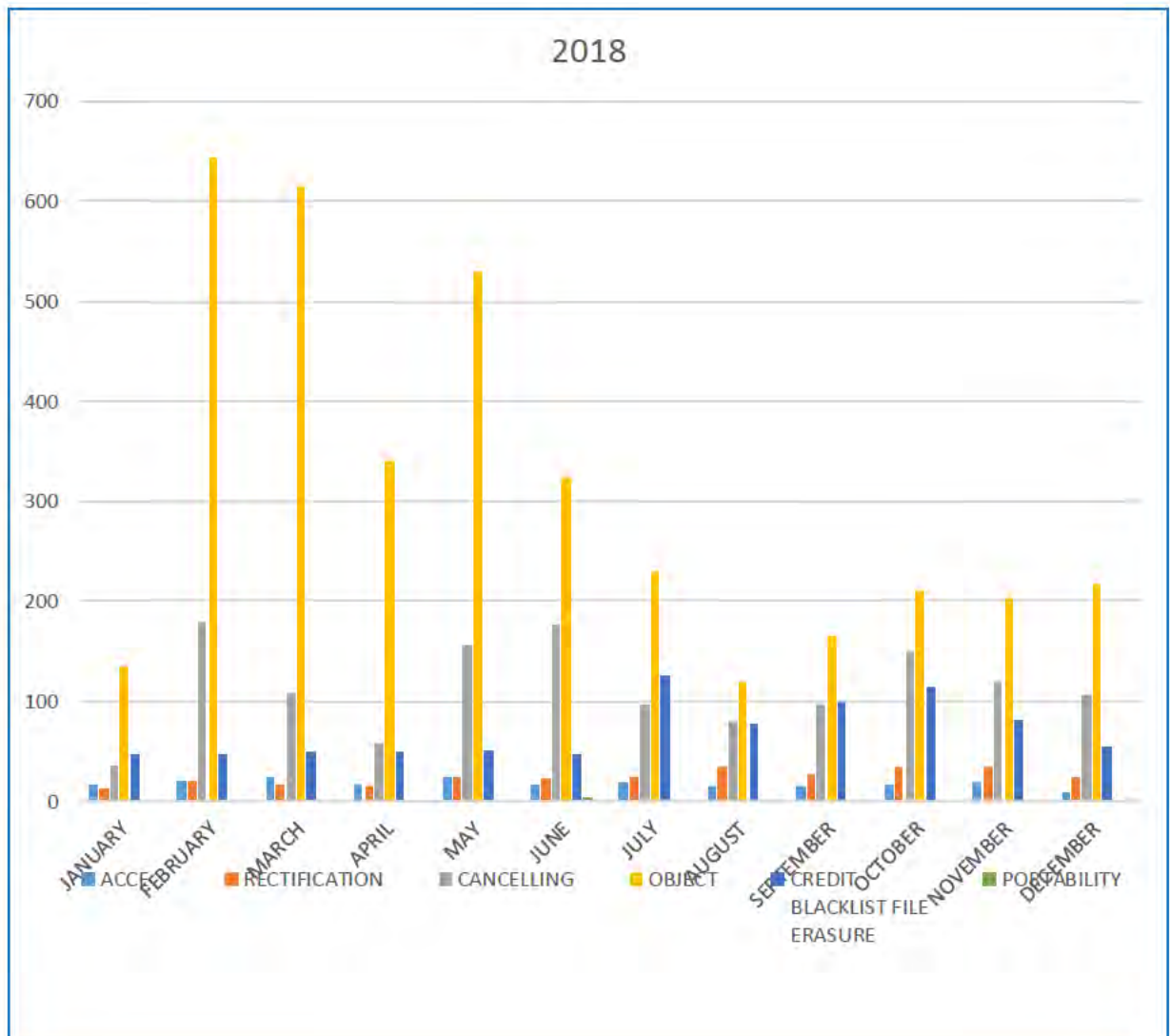
6417

2021	ACCESS	RECTIFICATION	ERASURE	OBJECT	CREDIT BLACKLIST FILE ERASURE	PORTABILITY
JANUARY	41	28	189	192	231	0
FEBRUARY	38	38	265	240	190	1
MARCH	76	37	231	564	121	2
APRIL	71	38	211	489	104	1
MAY	71	24	208	24	145	0
JUNE	89	19	187	128	99	1
JULY	28	17	263	142	151	0
AUGUST	44	25	155	107	118	0
SEPTEMBER	27	37	215	112	120	0
OCTOBER	19	32	169	112	175	1
NOVEMBER	35	48	234	128	181	0
DECEMBER	42	38	182	59	130	0
TOTAL	581	381	2509	2297	1765	6

7539

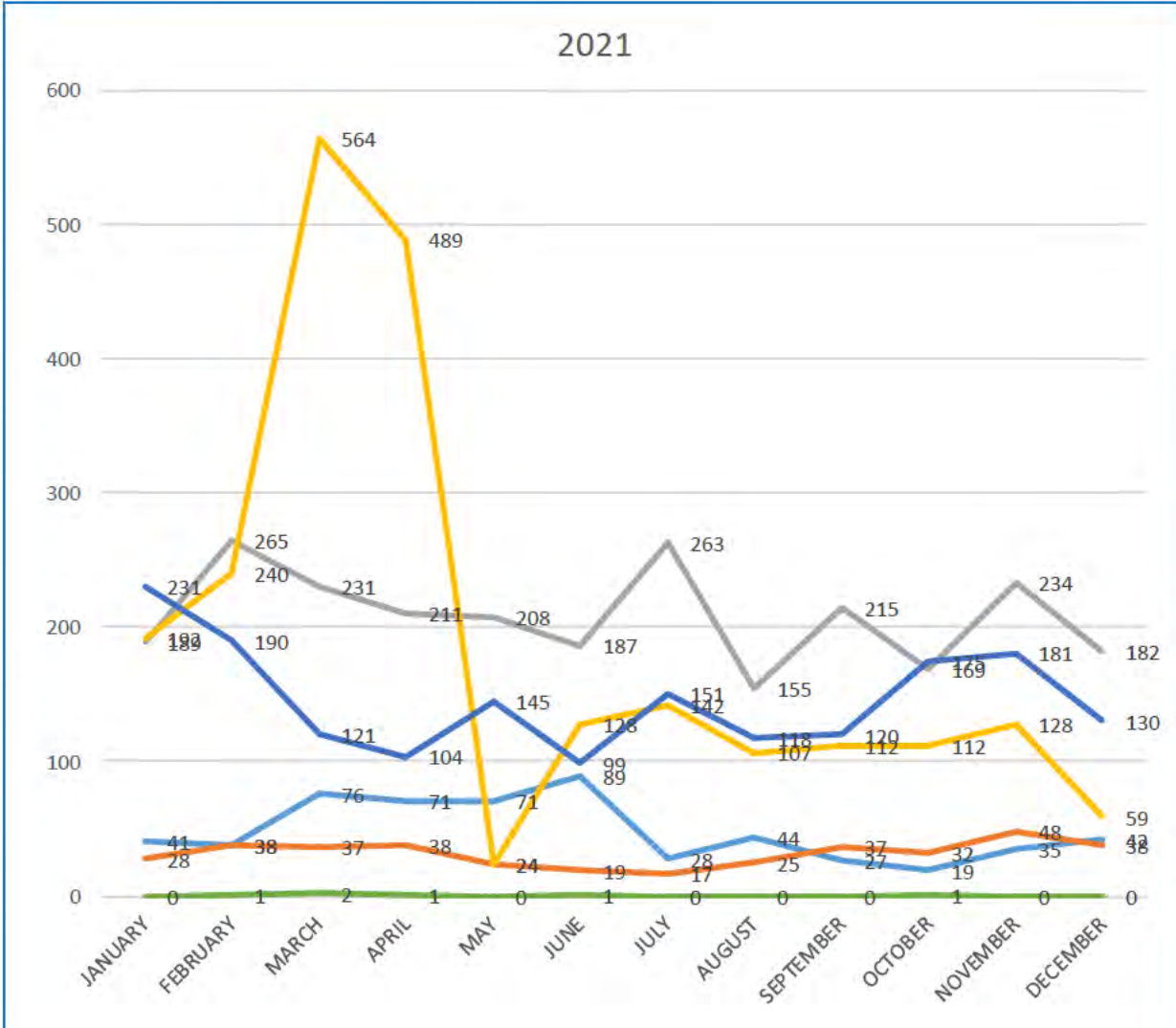
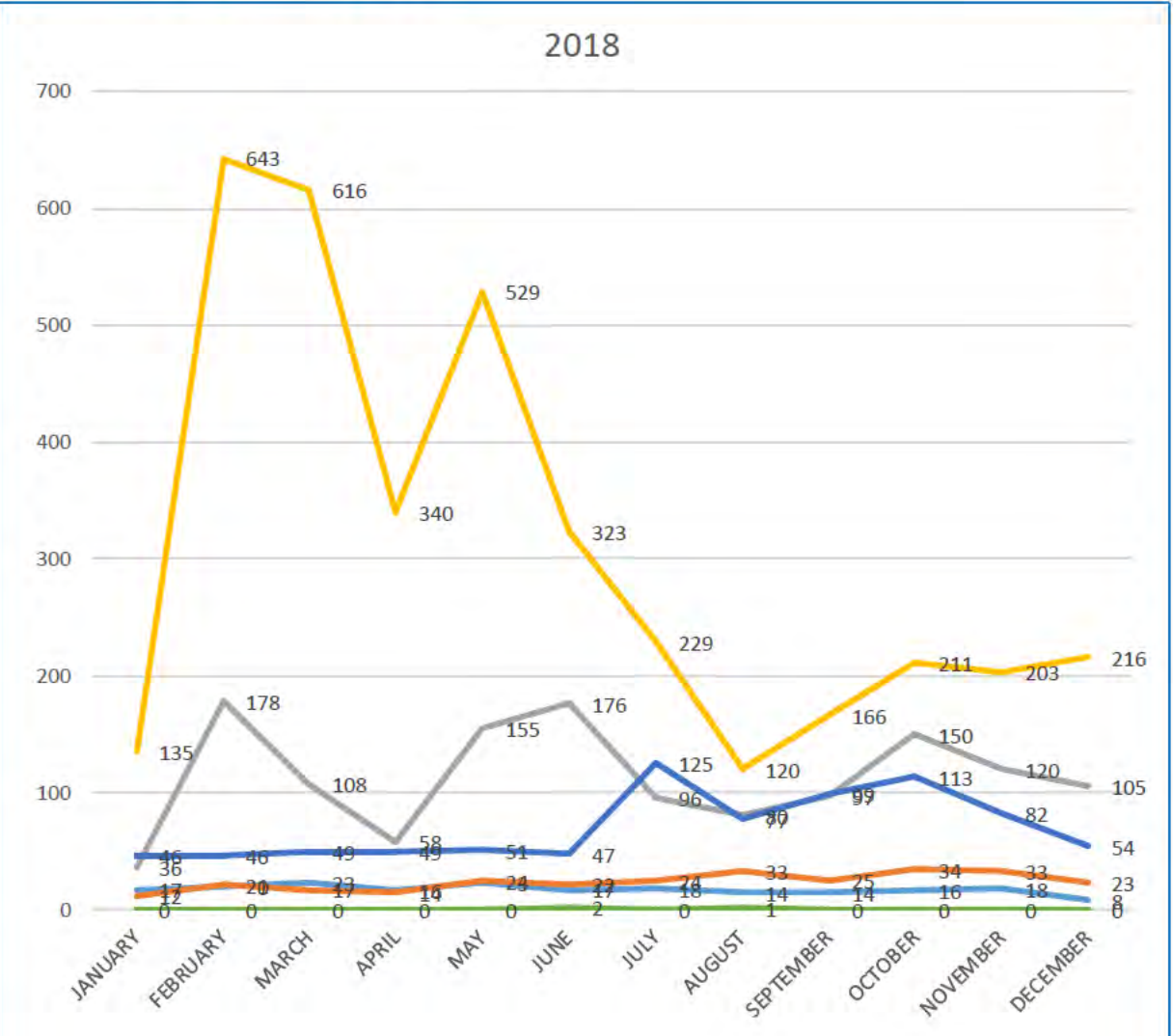
03 Type, volume & tipology

Statistics (II)



03 Type, volume & tipology

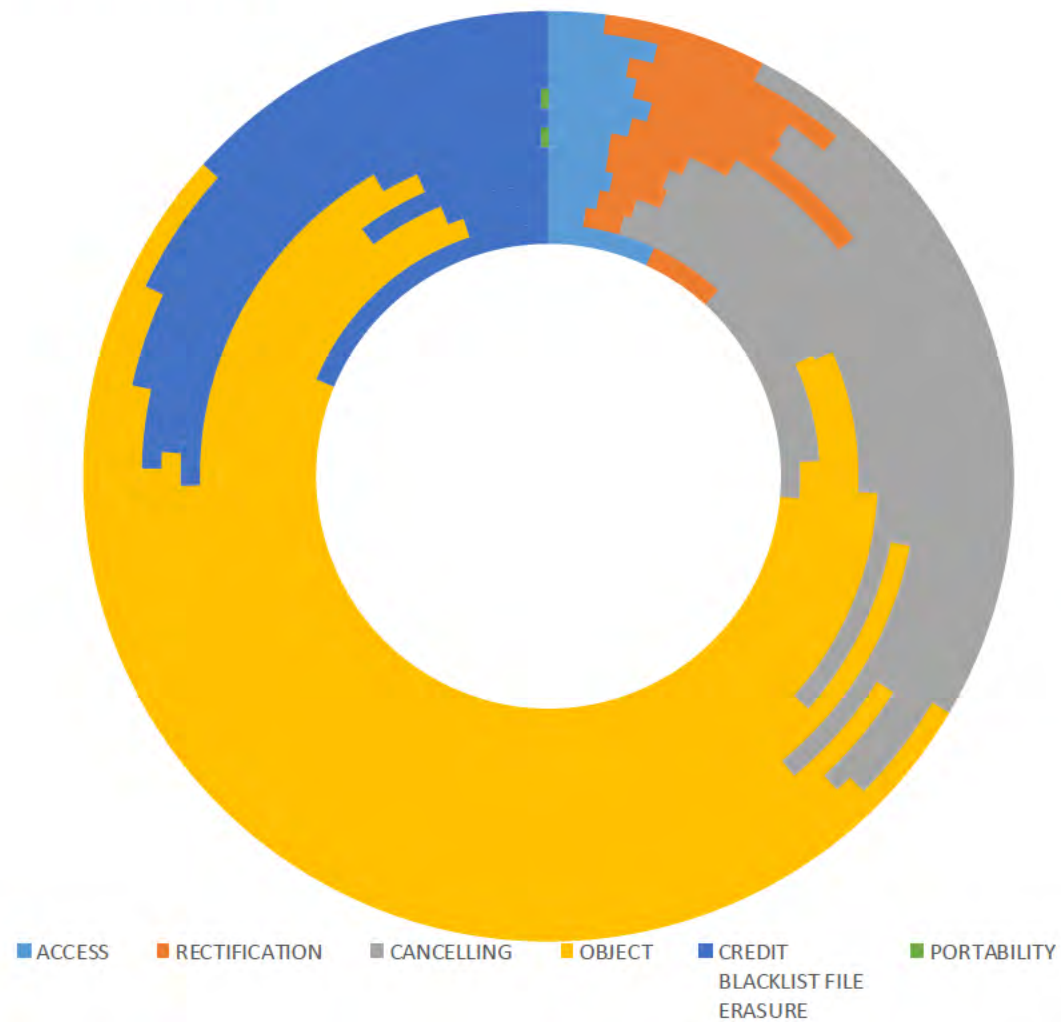
Statistics (III)



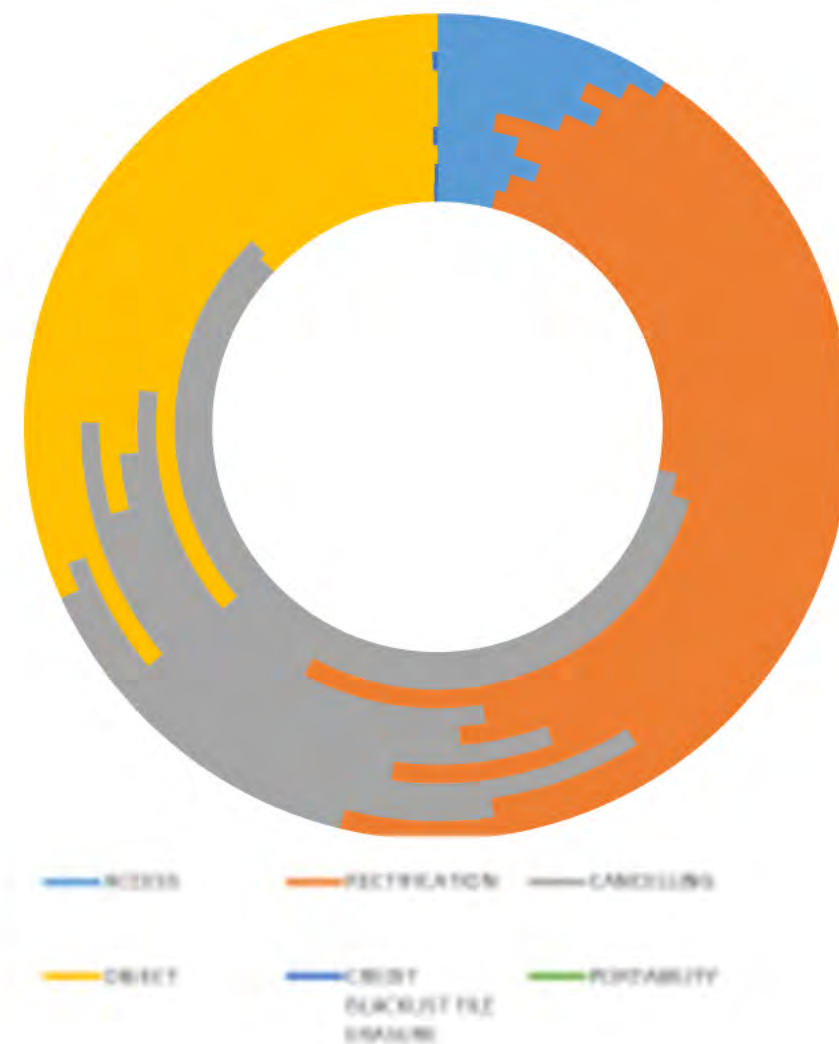
03 Type, volume & tipology

Statistics (IV)

2018



2021



04 Curiosities

Curiosities (I)

- Before GDPR was fully in force, well ahead of other companies, we sent a massive communication to fulfill with the right to be informed. Some clients answer back:
 - Some said they prohibited us to use data processors - providers. We have to clarify that they are not entitled to that.
 - Others prohibited to us to do any international transfer of personal information (TID), so, again we clarified they are not entitled to ban such possibility to us, as long as we comply with the requisites stated in GDPR to do that.
- There was an employee who wanted to exercise the right to erasure his personal data. I told him ... do you want to get paid by the end of this month? You'd better withdraw your request.



04 Curiosities

Curiosities (II) 😊

- A couple of cases where data subjects exercised the right to rectificate its own information because they changed their sex, from male to female and vice - versa.
- Most clients think the right to restrict processing is indeed the right to object. So when they exercise such right, we have to ask them what they mean, as its quite confusing. Only 1 so far was doing it well.
- Most clients believe the right to access means to provide them with documents, contracts, emails... or video surveillance and audios without even saying when they took place or if such videos or audios exist at all! Moreover, some believe this right allow them to request the name of the ██████████ employees who have had Access to their personal information.