



Rights of data subjects - an overview -

1. Definitions + principles
2. Individual rights + examples
3. Exceptions

Ute Kallenberger
DPO Training
17 April 2013

Strategy

2013-2014

“Data subject”

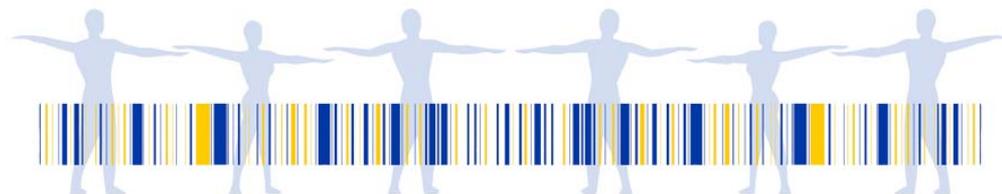
= the person whose personal data are collected, held or processed.

Broad scope of entitled individuals!



Recital (7) of the Regulation reads "*The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever...*"

Recital (5) of the Regulation stipulates that: "*A Regulation is necessary to provide the individual with legally enforceable rights...*"



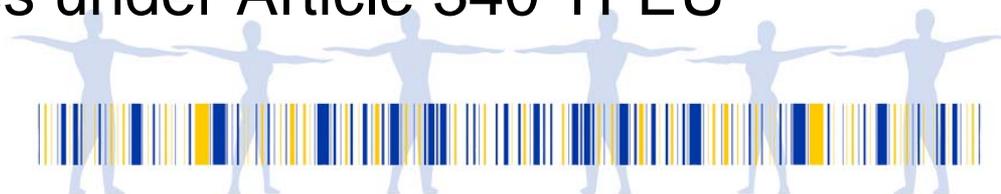
General vs specific rights

- **General right:** EU institutions and bodies must process personal data fairly and lawfully, and only for legitimate purposes (Articles 4 to 6 of the Regulation).

- **Specific rights** complemented the general right above (Sections 4 + 5 of the Regulation)

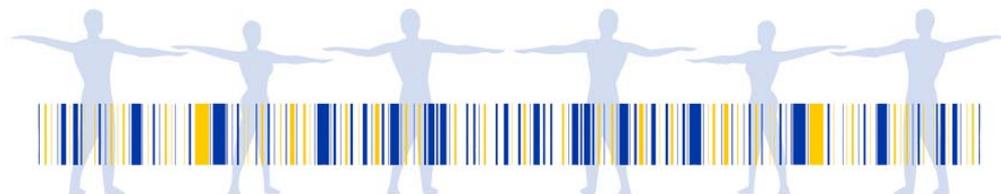
***These specific rights are
what this presentation is about***

- Since data subjects' rights constitute rules of law conferring rights on individuals, non-contractual liability for the breach of such rules under Article 340 TFEU



Data subject rights

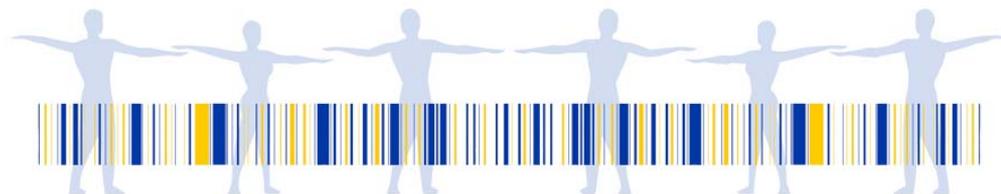
- Right of **information** (Section 4);
- Right of **access** (Article 13);
- Right of **rectification** (Article 14);
- Right of **blocking** (Article 15);
- Right of **erasure** (Article 16);
- Right to **object** to the processing (Article 18);
- Special rights in case of automated individual decisions (Article 19).



Common principles (1)

- DS rights shall be available at all times;
- Positive obligation to act for the controller and to guarantee their effective exercise;
- Within a reasonable time limit
 - “Without delay” for rectification
 - Promptly for blocking and erasure
 - “Within 3 months” for access

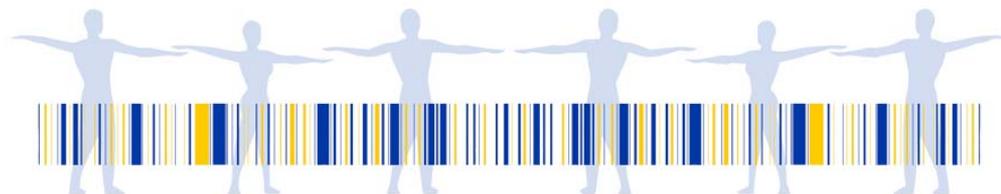
Internal procedure: Implementing rules concerning the tasks, duties and powers of the Data Protection Officer, Article 24(8)



Common principles (2)

Example: Positive obligation to act for the controller

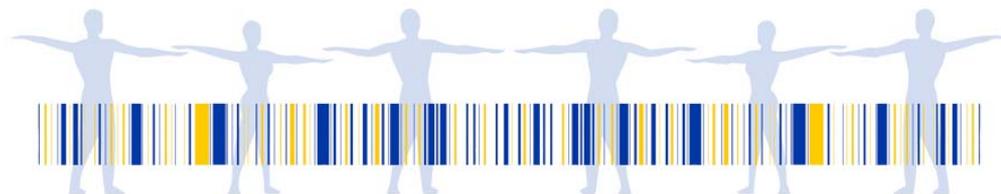
- Temporary staff: rights of access and rectification not attributed to the data subjects concerned, but limited to their employment agency;
- Obligation for EU body to ensure that the temporary staff themselves (not only their employment agency) can effectively exercise their rights under Articles 13 and 14.



Common principles (3)

Example: *Controller must ensure that the data subject can make effective use of his/her rights*

- Database containing evaluation results, *informal process* for data subjects to contest expert group assessment; *up to expert group* to re-evaluate and remove any mistake from the database.
- EU institution must clearly inform the data subjects of their rights to contest the accuracy of the data and to rectify them.

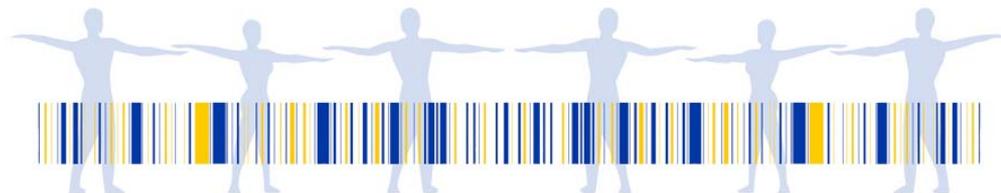


Common principles (4)

The mere citation of rights is insufficient.

The data subject is entitled to receive adequate information on how these rights are guaranteed and which limitations apply.

> *Privacy Statement*





Data subject rights + examples

Always

- **Information** (Arts.11+12);
- **access** (Art.13)

Inaccuracy or unlawful processing

- **rectification** (Art.14);
- **blocking** (Art.15);
- **erasure** (Art.16).

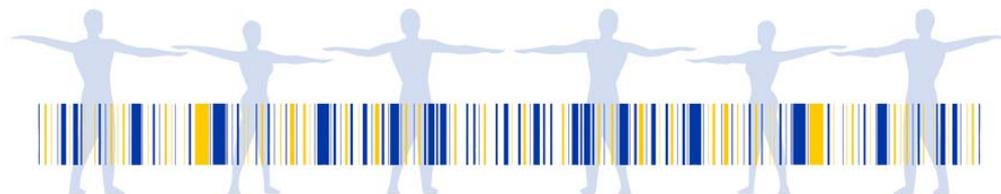
Compelling legitimate grounds

- **right to object** to processing (Art.18).



Right to be informed (1)

- **Articles 11 + 12 = “shopping list”**, depends on whether data obtained from data subject or not;
- obliges the controller to provide information on e.g. the identity of the controller, the purpose of the processing, the recipients of the data and the rights of the data subjects
- Information before first time disclosure to third parties (> right to object to such disclosure);



Right to be informed (2)

Example: *Recruitment question on "Interests & skills unrelated to work, including social and sport activities"*

Adds to knowledge of applicant, but not fully appropriate for the purpose of the application form.

Therefore, EDPS recommends

- 1) including this question only as optional in the application form;
- 2) ensuring that applicants not answering optional question will not be put to any disadvantaged position due to their failure to give answer.

> Obligation to inform applicant of 1) + 2)



Right to access (1)

The data subject is entitled to receive

- within three months from receipt and
- free of charge:



- **confirmation** as to whether data related to him or her are being processed;
- **information** on purposes, categories of data, and recipients;
- **communication** in an intelligible form of own data undergoing processing;
- **logic behind** any automated decision process concerning him or her.



Right to access (2)

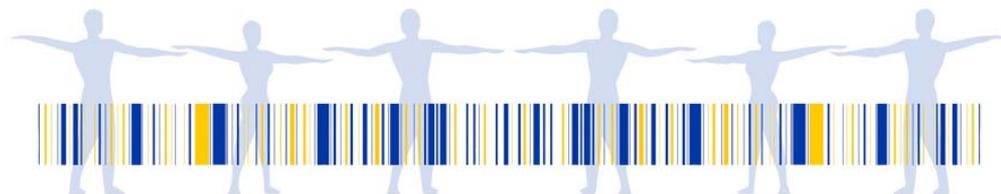
- Access granted **to the fullest extent**, as it helps to
 - understand which data are processed about him/her;
 - verify the quality of his/her own data;
 - verify the lawfulness of the processing;
 - exercise his/her other data protection rights.
- **Unless** an exemption under Article 20(1) applies:
 - narrow interpretation, on a case-by-case basis;
 - must not be restricted more broadly than necessary.



Right to access (3)

Examples:

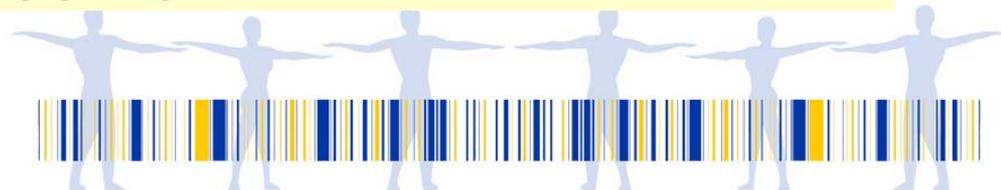
- **Format of the data:** usually access is granted by providing paper copies or electronic copies. Sometimes, need to adapt to the data subject, e.g. the case of a blind person who needs electronic copies.
- **Intelligible form:** right to access meant to enable data subjects to control the quality of their personal data and the lawfulness of the processing. E.g. medical practitioner must interpret the data (such as blood analysis) and/or make the data decipherable.



Right to access (4)

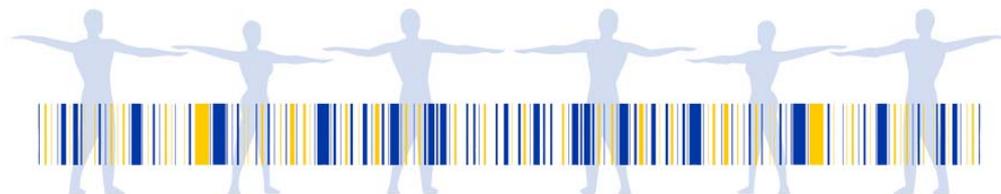
Example: *Selection procedures (pre-selection tests, interviews and written examinations)*

- Data subjects should in principle be given access to their evaluation results regarding **all stages of the procedure**.
- Possible exception under Article 20(1)(c) in line with Staff Regulations ("*The proceedings of the Selection Board shall be secret*" – independence jury, rights of other candidates).
- Data subjects should nonetheless be provided with evaluation **criteria** and **aggregated results**.



Rights triggered by inaccuracy or unlawful processing

- **Inaccuracy / incompleteness:**
 - right to rectify or to block the data until the controller has verified the data;
 - rectification of objective and factual data;
 - completeness of file: complementary documents may be added, data subject has the right to express his/her point of view;
- **Unlawful processing:** right to erase data or to block them.



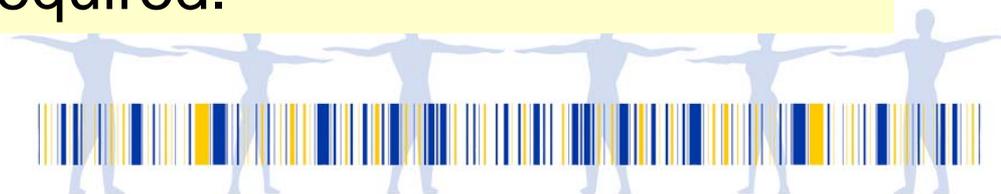
Unlawful processing

Unlawful because there is no legal basis under Article 5 of the Regulation or because there has been a breach of the Regulation by the controller.



Example: Asset freezing

- Review procedure concludes that initial decision to list a data subject was unlawful (wrongfully listed): additional measures on top of a simple removal from list required = publicly "clear" the names of wrongfully listed persons;
- Impossible to remove from Official Journal once published; corrigendum required.



Right to rectify (1)

Only applies to objective and factual data; subjective statements by definition cannot be factually “wrong”. In certain cases, right to complement existing data with a second opinion or counter expertise.

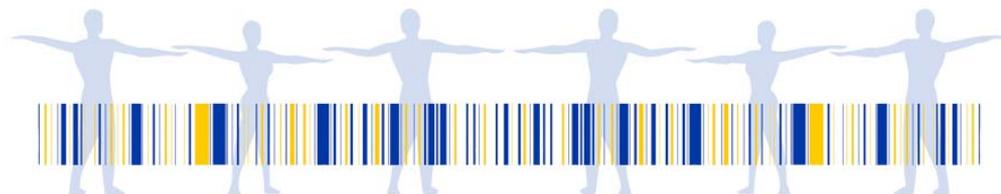
Example: *Informal procedure for the prevention of psychological and sexual harassment*

Distinction objective/hard data vs subjective/soft data; rectifiable inaccurate "soft data" can only relate to the fact that specific statements have been made by the data subject. To ensure completeness of the file, data subjects may add their opinion.



Right to block

- Privacy by design: foresee possibility to block individual data without blocking the whole system!
- Two situations need to be distinguished:
 - 1) **Accuracy** contested: data must be blocked immediately for the period necessary to verify the accuracy and completeness of the data.
 - 2) Request to block is based on grounds of **unlawful processing** or where the data must be blocked for **purposes of proof**: Controller must conduct assessment; “as quickly as possible, at the latest within 15 working days”.

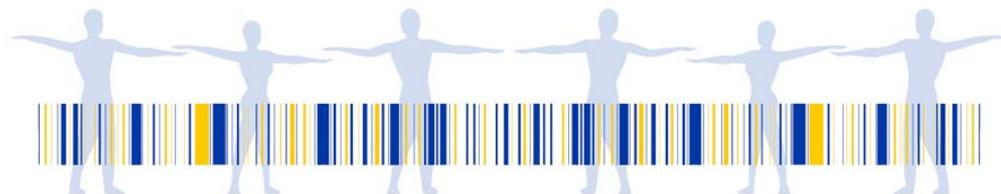
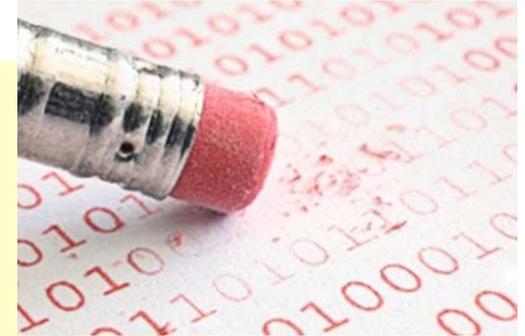


Right of erasure

Example: Administrative inquiries and disciplinary proceedings

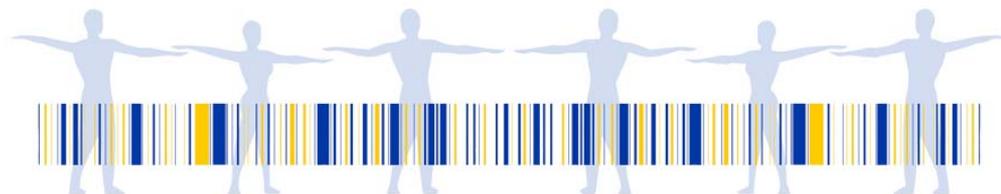
Article 27 of Annex IX to the Staff Regulations: removal from personal file at discretion of Appointing Authority; Data subject is not granted automatic removal.

Contradicts the principles set out in the Regulation; Fairness of data processing would imply justification why data are being kept and of refusal to erase data where the data subject so requests.



Right to object (1)

- Triggered by particular situation of data subject:
“**compelling legitimate grounds**”;
- Where data subjects have previously given their **consent** under Article 5(b), this **does not exclude** the subsequent exercise of the right to object. The EDPS considers that for consent to be “freely given”, withdrawal should always be made possible;
- Part of the recommended proactive approach on public access to documents.



Right to object (2)

Examples:

No compelling legitimate ground:

- Objection of publication of name in Tendering Register of the EU (TED) as contact person;
- Objection in context of civil proceedings that COM discloses information to a third party on whether or not a data subject was a civil servant at COM;
- Objection to disclosure of the salary data to the spouse in context of divorce procedure.

Compelling legitimate ground:

- Objection to publication of name of data subject mentioned in decisions by national courts published on the internet.



Exceptions, Art. 20

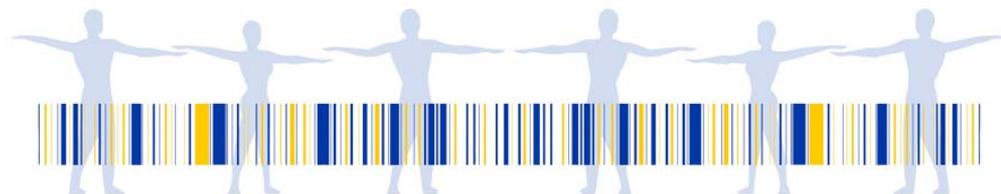
Article 20(1): “...*necessary measure to safeguard:*

(a) the prevention, investigation, detection and prosecution of criminal offences;

(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;

(c) the protection of the data subject or of the rights and freedoms of others;

(d) the national security, public security or defence of the Member States; ...”

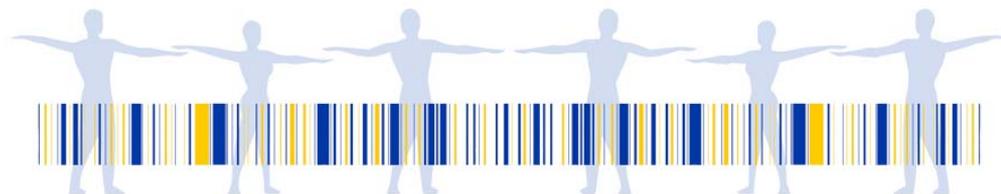


Right to access (4bis)

Example: Selection procedures (pre-selection tests, interviews and written examinations)

- Principle (see above): access to evaluation results
- Possible exception under **Article 20(1)(c)** to protect
 - the independence of the jury;
 - the confidentiality of the jury's deliberations;
 - decision-making of Selection Committee / individual members;
 - safeguard the rights of other candidates.

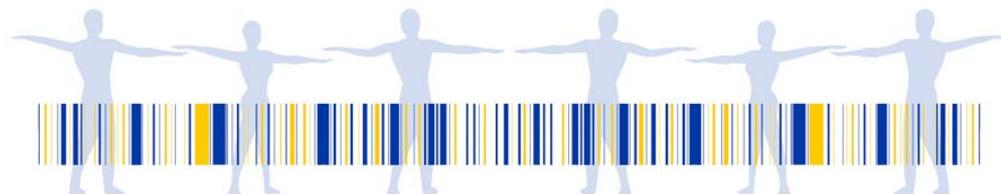
But: Data subjects should nonetheless be provided with evaluation **criteria** and **aggregated results**.



Right to access (5)

Example: Harassment

- Alleged harassers may have their right to access restricted if necessary to safeguard "*the protection of the data subject or of the rights and freedoms of others*", **Article 20(1)(c)**;
- Access is subject to them having been informed by the controller, with the agreement of the alleged victim, of the existence of an informal procedure against them;
- Article 20(1)(c) also applicable to protect the rights of other persons concerned, especially of witnesses.



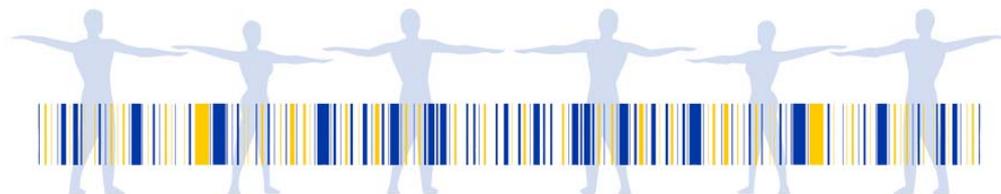
Right to access (6)

Example:

Access certain medical data through a doctor

Psychological or psychiatric data

- case-by-case assessment: no direct access can be given in order to protect *the data subject* based on Article 20(1)(c);
- In such cases, EU administration should ensure that data subjects have indirect access.

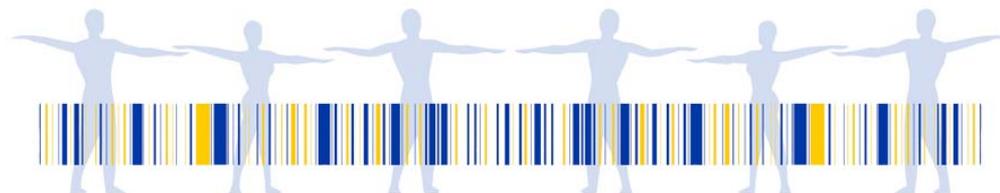


Right to rectify (2)

Example: Grant and procurement award procedures

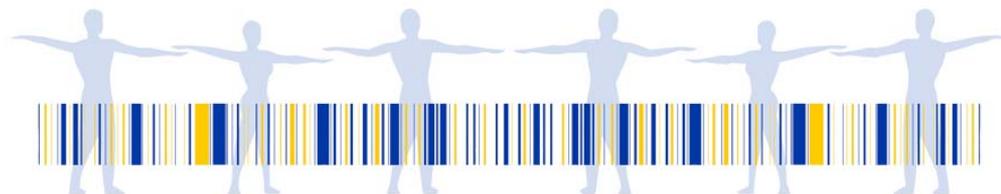
Data subjects are granted rights of access and rectification upon request, but the right to rectify is limited and can only be exercised up to the closing date for submission of applications or tenders.

The EDPS considers that this limitation of the right to rectify could be considered as justified in light of **Article 148(3) of the Financial Regulation** aiming to ensure transparency and equality of treatment and thus compliant with **Article 20(1) (b) + (c)**



Article 20(2)-(5)

- **Article 20(3)** obliges the controller to **inform** the data subject of the principal reasons for deferring access and the right to seek recourse to the EDPS;
- **Article 20(4)** establishes that, when investigating complaints by data subjects in such cases (*indirect access*), the EDPS shall only **inform** the data subject whether data have been processed correctly and if not, whether the necessary corrections have been made;
- **Article 20(5)**: this **information may be deferred** as long as it would deprive the restriction imposed under Article 20(1) of its effect.



Article 20(2)-(5)

***Example:** Administrative inquiries and disciplinary proceedings*

- **Witnesses** in principle: no confidentiality required. However: case-by-case analysis.
- Identity of **whistleblowers and informants** is kept confidential, unless infringement of national rules on judicial procedures and/or malicious false statements.
- Vulnerability of whistleblowers and informants remains the same **after closure** of investigation. Risks to privacy and integrity independent of whether investigation is opened or closed with no follow-up.



Thank you for your attention!

Do you have any questions?

For more information:

www.edps.europa.eu

edps@edps.europa.eu



@EU_EDPS

Strategy

2013-2014