EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The Restaurant at the End of the Universe

Case Study
Event Management

✓ All events described in this exercise are purely fictitious.

✓ Any similarity to actual persons or facts are merely coincidental.

✓ This is based on best-practice examples the EDPS *already knows* about... There might be more!

Scene setter

- Your EUI plans a big event on *(insert your EUI's core business activity)* with various external stake-holders and participants from your and other EUIs.
- Your EUI already has e-mail addresses for some participants (newsletter subscribers, participants in past events) and your colleagues have found more e-mail addresses of potentially interested external stakeholders on the internet.
- An external contractor will be in charge of the overall organisation of the event (taking pictures, registration of visitors, catering etc.).

Your role

- You are asked by your Head of Unit to coordinate this event on the side of your EUI. Congrats!
- In particular, he asks you to collect the following, so he can send this to the external contractor:

  - confirmation of attendance of the identified potential participants;

  - a copy of their ID cards to facilitate registration and since it may be useful at a later stage;

  - their nutritional allergies and preferences for planning by the caterer.
- Your DPC and your DPO are on holidays...

Your mission

Please get together in small groups.

At each step consider first amongst yourselves what the answers might be.

Then share with all.

Your participants

Your efforts in marketing the event have been successful and your inbox has been busy lately:

- One third of the potential participants identified on the internet came back informing you that they are interested in participating in the event;

- One third informed you that they are not interested;

- One third did not reply at all.

Question 1: Your participants

How do you proceed?

- During first contact: provide specific data protection notice, incl. source of personal data, legal basis...

  Arts. 14-16 Reg

- Those not replying and those not interested should be deleted from future event correspondence, since not necessary to keep their data.

How about persons whose contact details were *already known* to your EUI (not identified via internet)?

- Specific consent might be required – depending on what they consented to in the past. Arts. 3(15), 7 Reg

Consent

- Art. 3(1)(15): “...any **freely given**, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to him or her; ...”;
- Art. 7(1): controller: obligation to demonstrate;
- Art. 7(2): distinguishable and transparent;
- Art. 7(3): consent as easy to withdraw as to give;
- Art. 7(4): not freely given, if tied / pre-condition for performance of contract;
- Art. 8: children

Art. 3(1)(15)Reg = Art. 4 No. 11 GDPR

“Clear affirmative action”?

“Your personal data will be part of a list of contact details shared internally for the purpose of contacting you in the future in the context of our activities.
If you do not agree with this, please contact the controller by using the contact information below and by explicitly specifying your request.”

“Clear affirmative action”!

“We would like to insert your personal data in a list of contact details shared internally for the purpose of contacting you in the future in the context of our activities.
If you agree with this, please tick this box: ☐ ”

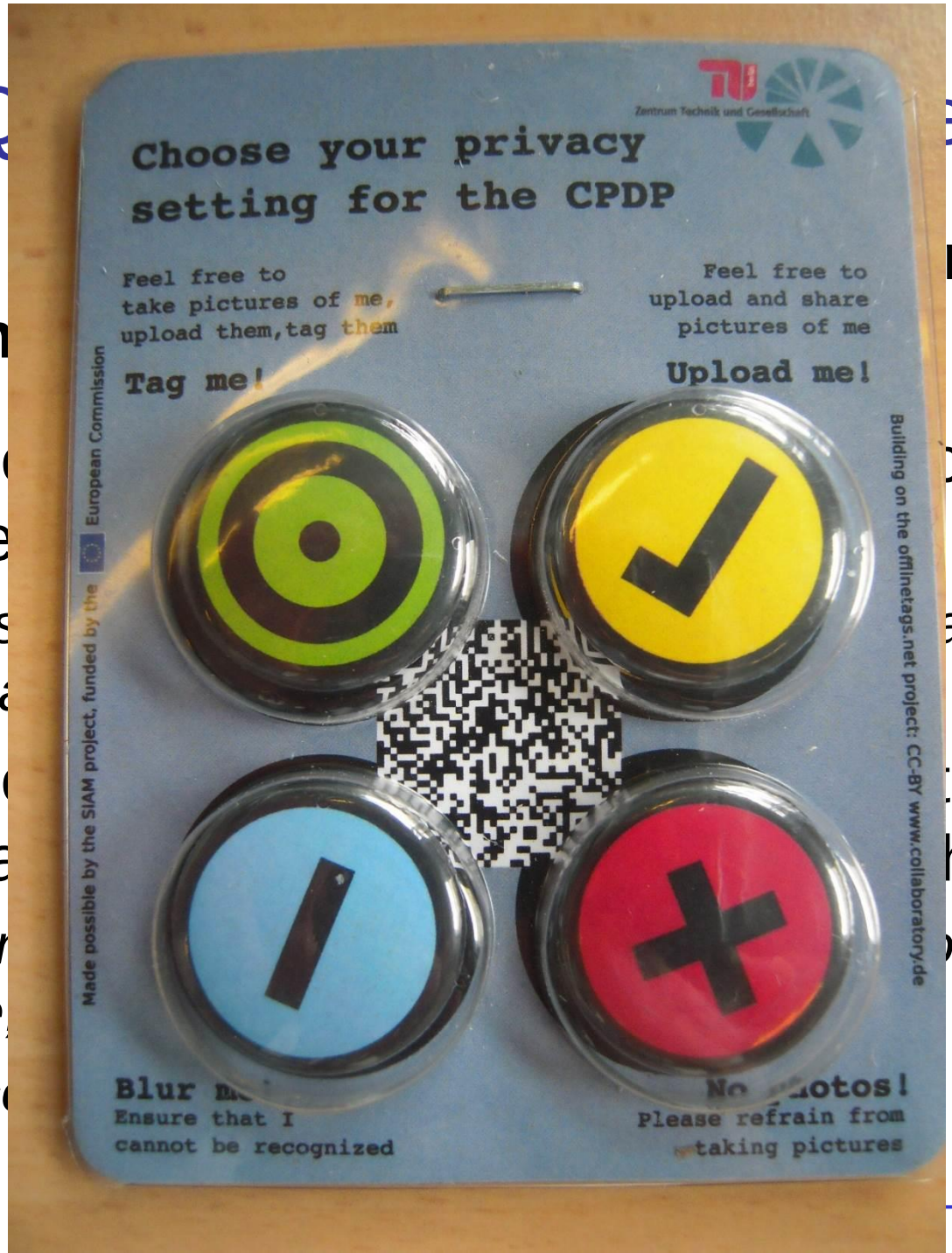
Art. 7(1): controller: obligation to **demonstrate consent**

Q…eos

Taking …m on the Intern… …r HoU?

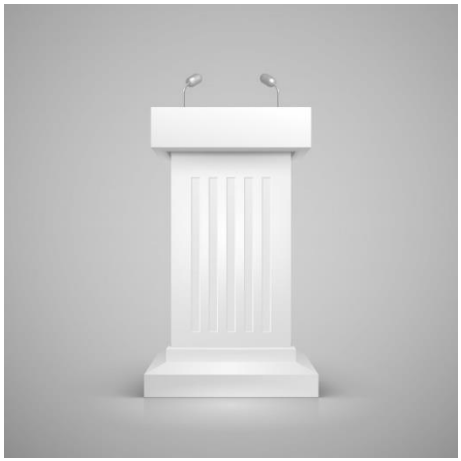
- Controll… …ction notice before e…
  - *purpos… …ation, right to withdra…*
- Controll… …t of each particip… …his consent
  - *Area i… …loured badge…*
  - *If no c… …taking.*

…15), 7 Reg



Your speaker

One of the experts you invited as a speaker informs you that she is surprised that your EUI contacted her. She asks you to provide her with a copy of all data that you have about her and to immediately delete those data.



Your Head of Unit says there is no problem to delete her data, but that it is not necessary to do a cumbersome research since the problem is now solved with their deletion.

Question 3: Expert / speaker

What do you advise?

- Her right of access to her personal data means you need to provide a copy of all her personal data. Art. 17 Reg.
- Comparatively easier if your EUI held that info centralised (think: PbD...); otherwise this implies researching many different excel tables kept by different colleagues...
- Right to erasure, since no legal basis for your EUI to keep her data and since person did not consent. Art. 19 Reg.

Copies of ID cards

You remember that your HoU asked you to collect a copy of each participant's ID card to facilitate their registration and since it may be useful at a later stage.

Question 4: ID card copy

Would you consider it necessary and proportionate to require a copy of their ID card? **Why?**

Question 5: Retention periods

How long will you keep the participants' personal data?

- Up to you to determine necessity: Keep only as long as "necessary".
- Define retention period and distinguish between categories of data (contact details vs allergy data vs ID number).
- No keeping "just in case".

Art. 4(1) Reg

Question 6: Catering

How will you transfer participants' data as to their nutritional allergies and preferences?

How long will you keep this information?

- Safeguard clause in contract.

- Confidentially reminder in email by which you send the information.

- In your Unit and the company to be deleted after event (no longer necessary!).

Your participants list

(Insert name of important private sector stakeholder here) wishes to organise a similar but more restricted event some weeks after your EUI's conference. They ask your EUI if they can have access to the participants list.

Your Head of Unit indicates that this request is a top priority for him, a mere recycling exercise for you and you should send the list without delay.

Question 7:

What do you advise?

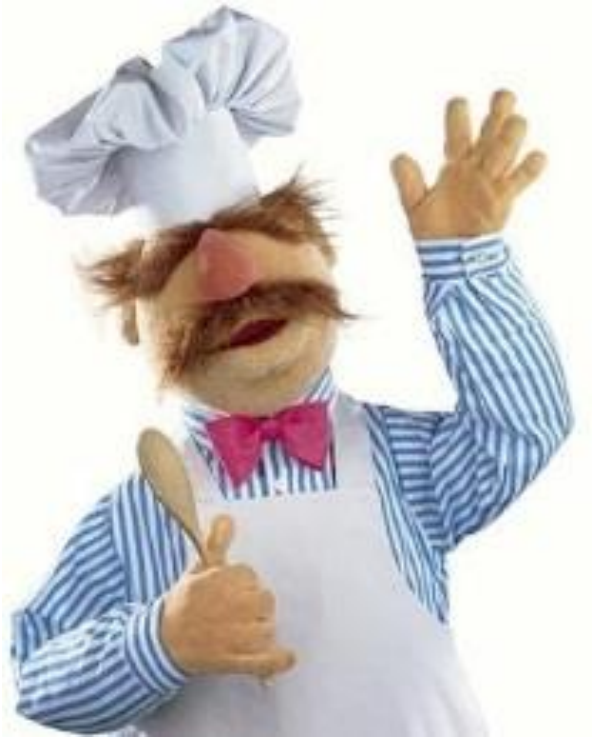
- The *important private sector stakeholder* would need to establish necessity. Here they could establish their own list of experts, so the transfer is not “necessary”.

***Alternative:* Would the situation be different if an MEP asked for this list?**

- No, same rules apply!

Your participants list

One week before the event the external contractor informs you that the cook had a printed copy of all participants with allergies or special dietary requests. When the cook visited the event location in order to prepare the catering, he lost this list in the subway.



Your Head of Unit is quite upset with the company, but says it is not your EUI's problem.

Question 8:

- This
- This
- Cons

eed to be re Art. 34 Reg

DPC even e able to pr o.

about this. Art. 35 Reg

Question 9: Mass emailing

Your HoU asks you to send practical information about the event to all participants. How do you proceed?

- Put participants in ***bcc***; the other participants do not need to receive all other email addresses.
- Transfers should occur on a need-to-know-basis.
- Assess the need-to-know of each recipient: is the e-mail relevant and necessary to be disclosed? ...for which purpose?
- Avoid disclosure of data to unauthorized persons (caution: auto-complete...)!

thank you!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

 **@EU_EDPS**

 **EDPS**

 **European Data Protection Supervisor**

Right of access (Article 17)

Art.14

What

- processing? Y/N, purpose, categories, source, recipients, incl. 3rd country ones, automated decision-making
- Art. 17 = “shopping list”

NEW

Format

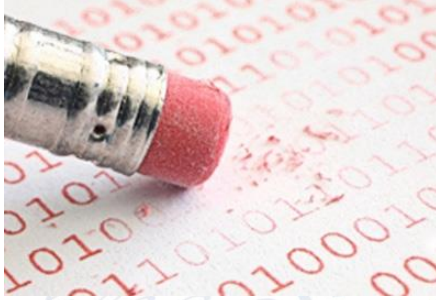
- controller shall provide **copy**
- commonly used electronic form

NEW

and...

- no copy if adversely affects rights and freedoms of others

Right to erasure (Article 19) ('right to be forgotten')



What

- *right* to erasure without undue delay
- *obligation* of controller

public

- technology / cost / reasonable steps
- inform controller of links/copies/replica

except

- no erasure if necessary for freedom of expression, legal obligation, public health, archiving, legal claims

NEW

Right to be informed / source not DS (Article 16)

When

- within reasonable period / max. 1 month
- unless the DS already has the info or
- impossible / disproportionate effort (scientific purposes)

NEW

What

- Art. 16 = “shopping list”, incl. EDPS
- DPO, 3rd country and safeguards, right to withdraw consent, existence of automated decision making, EDPS
- Source of PD / whether publicly accessible

and...

- further processing: prior info required
- Recital 28: standardised icons

NEW

Case Study
Event Management

Ute Kallenberger, EDPS

DPO Meeting

EIOPA, Frankfurt/Main, 17 May 2019

Your external provider

From: EUI procurement unit
Sent: 17 May 2019 10:00
To: YOU
Subject: Your event on our EUI's core business activity

Dear colleague,

Given the high number of participants, we will need to rely on an external contractor. The cheapest one is established in Member State A.

As standard service, they offer the services of one of their photographers and publication of the pictures on their website after the event. It seems that some of their datacentres are located with Amazon in the USA.

Please confirm that this is OK with you.

Have a great day,

...

Question X: External provider

Concerning the use of this external contractor, what should you consider?

- Call for tender: minimum requirement recommended: No data processing in non-EU/-adequate countries;
- Contractual safeguards (only authorised persons should have access, right to audit contractor, data should be deleted and returned to your EUI after the event etc. ...; see Article 29 of new Regulation);
- No sub-contracting by event company without prior authorisation by your EUI;
- Draft record & provide data protection notice.

Outsourcing

Privacy as award criterion: « *Procure secure* »

- Remember privacy by design & by default

Review, update and renegotiate contract clauses

- Clarify roles controller/processor
- Contractual safeguards (security, confidentiality)
- Processor should act only on behalf of the controller
- Privacy statements, no sub-sub-contracting...

Controller can verify compliance via audits

Art. 29 new Reg