# ERN CPMS 2.0
# DPIA Results and Next steps

## 29.04.2025 – Second Session

*European Commission*
*Directorate-General for Health and Food Safety*
*Unit B3 - Health monitoring and cooperation, Health networks*

# Practical and legal considerations

1. Identify yourself correctly: Affiliation – First Name Last Name
   Example: DG SANTE – Joao de Sousa (if necessary, right-click on your name and “Edit display name”)

2. Keep your camera open
   Keep your microphone muted when not speaking

The meeting is being recorded for the purpose of helping to write the minutes.
By attending you consent to being recorded.

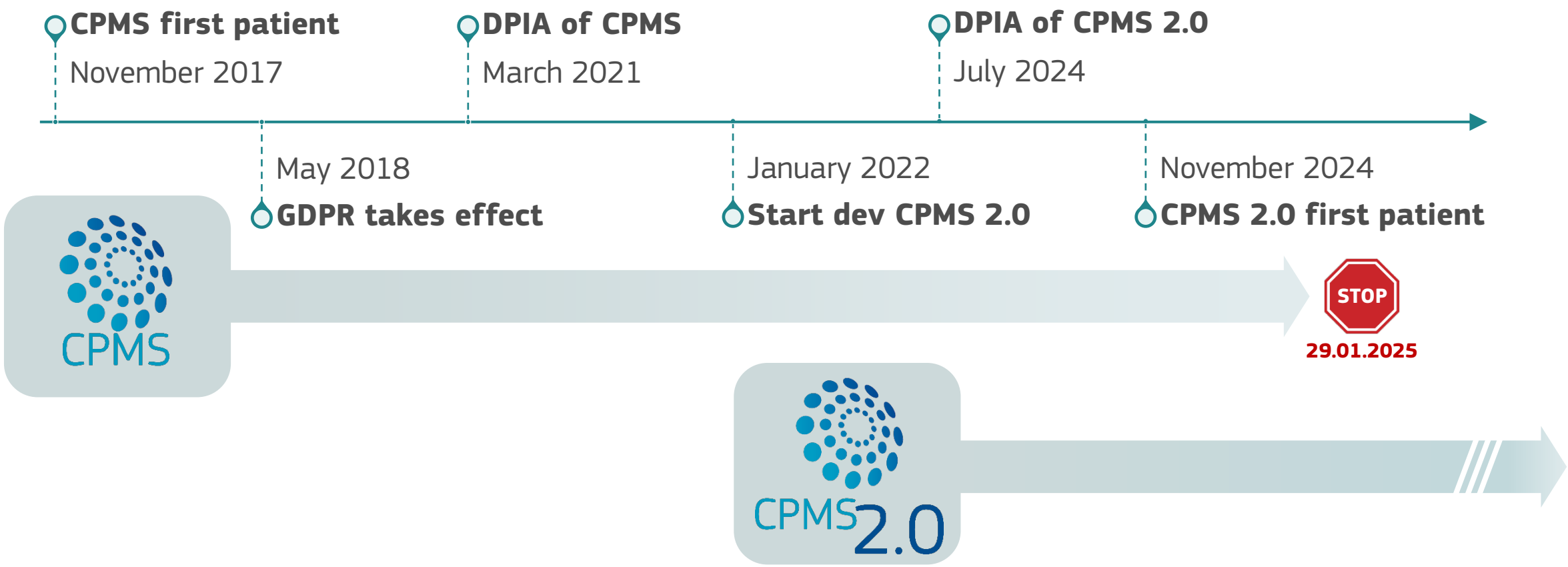
# Agenda

1. Introduction and context
2. DPIA presentation
3. Next steps for hospitals
4. Discussion
5. AoB and closing

# Clinical Patient Management System

- IT platform used in the context of general clinical practice
- Secure environment for cross border medical discussions
  - Sharing of patient cases
  - Audio, video and text interactions, including medical imaging

# Clinical Patient Management System – timeline






European Commission

# Clinical Patient Management System – legal base

- Article 12 of the Directive 2011/24/EU on the application of patients' rights in cross-border healthcare.
- Commission Implementing Decision (EU) 2019/1269, of 26.7.2019, amending Implementing Decision 2014/287/EU.
- Joint controllership: European Commission + Healthcare Providers

(Annex 1 of Implementing Decision (EU) 2019/1269)

# CPMS 2.0 Data Privacy Impact assessment (DPIA)

- Completed: July 2024, by Trasys International, NRB group
  - European Data Protection Supervisor guidelines
  - ENISA guidelines on Security of Personal Data Processing
- Result: CPMS 2.0 is fully GDPR compliant
- Recommendations: already implemented or being addressed

# CPMS 2.0 DPIA overview


- CPMS 2.0 Processes:
  - Identification and contact details of authorised user's
  - Identification and medical data of patients
- Risk threshold assessment:
  - Sensitive data
  - Vulnerable data subjects

# CPMS 2.0 DPIA initial assessment

- Lawfulness (article 5 of the EUDPR):
  - Tasks carried out in the public interest or in the exercise of official authority
  - Data subject consent
    - Users and patients informed by a Privacy Statement
    - Consent asked to users and patients
- Necessity:
  - Most effective means for the EC to fulfil its mandate of establishing the ERNs
  - Least intrusive option for remote collaboration

# CPMS 2.0 DPIA initial assessment

- Proportionality:
  - Implements the minimum workflow and features
  - Interferences are proportionate to the purpose of helping patients
    - Each interference is mitigated
    - The superior interest of the patient is the driving force of the platform

# CPMS 2.0 DPIA initial assessment

- Transparency:
  - CPMS 2.0 Privacy Statement available within the platform
  - Consent forms used by EU hospitals to collect patient consent
  - Special consent form used by UA hospitals to collect patient consent
  - Information is complete, easy to understand and targeted to the audience
  - Information is communicated before the data is processed

# CPMS 2.0 DPIA initial assessment

- Fairness:
  - Data subjects are informed and aware of the processing of their data
  - Freedom of consent and consent revoking. No consent-based discrimination
  - Easy to exercise data subjects' rights:
    - Users can withdraw their consent or remove their data directly on the platform
    - Patients can contact the correspondent healthcare provider using the contacts mentioned in the correspondent consent form.

# CPMS 2.0 DPIA initial assessment

- Purpose and storage limitations:
  - All purposes of the process are identified
  - Data is not re-used for other purposes
  - Retention policies are clearly defined:
    - User, discussion and transaction data – while user remains active.
      Reviewed after 5 years of inactivity.
    - Patient data - for the time required to correctly follow up the patient and his/her family needs.
      Need for keeping patient data evaluated by the concerned ERN at least every 15 years.

# CPMS 2.0 DPIA initial assessment

- Data minimization and accuracy
  - Data collected and processed is adequate and limited for purposes
  - Patient data is pseudonymised. A unique ID is automatically created by the platform when a new patient is enrolled
  - Users entering data must ensure data is accurate and up to date
  - Inaccurate data can be deleted or rectified at any moment

# CPMS 2.0 DPIA initial assessment

- Transfer to third country – Ukraine (UA)
  - Administrative agreement signed with Ukraine
  - Ukraine patient cases may be discussed in the CPMS 2.0 system
  - Outcome report of a patient discussion accessible to UA clinician participants
  - Report includes names and affiliations of all participants who explicitly consent to the transfer

# CPMS 2.0 DPIA - security and data protection risks

- Risks were analysed (scale of 1-16) based on relevant guidelines
  - Risks related to the security protection of personal data.
  - Risks related to the non-compliance with EUDPR/GDPR principles
- Conclusion: all risks are acceptable (highest residual risk level was 4)

# CPMS 2.0 DPIA – security and data protection risks

- Insufficient protection resulting in:
  - health information disclosure or manipulation
  - systems unavailability and/or health information loss
- Incapability to sufficiently and timely manage security breaches
- Insufficient protection provided by the security measures
- Insufficient security governance
- Personal data merged or included in external systems
- IT systems being used by external malicious actors
- Insecure systems and practices
- Users' activities tracking

- Unfair processing of personal data
- Unavailability of transparent information on personal data processing
- Personal data processing for different purposes
- Unnecessary personal data processing
- Processing of inaccurate personal data
- Extended storage of personal data

# CPMS 2.0 DPIA – recommendations

| Recommendation | Status of implementation |
|---|---|
| Coordinate with and support HCPs, if needed:<br>1. Development of acceptable use policy<br>2. HCPs DPIA and security awareness of users | SANTE to periodically discuss with HCPs on best practices |
| 3. Establishment of a user access management process based on EC standards | Integrated in the platform |

# CPMS 2.0 DPIA – recommendations

| Recommendation | Status of implementation |
|---|---|
| 4. Holistic and full-scale penetration tests executed by an independent party | Included in the acceptance workflow of each major release |
| 5. Development of a disaster Recovery Plan<br>6. Planning and execution of annual Business Continuity and disaster Recovery tests | Both covered in the yearly contracts with the solution provider (IBM) |

# Next steps for HCPs

1. Mandatory - HCP decision about the patient consent form (PCF)
    - Continue using the current CPMS PCF (first consent only)
    - Adapt the EC-provided CPMS 2.0 PCF template
    - Use a different PCF
2. If deemed necessary – Data Privacy Impact Assessment of the processing activities under HCP responsibility

# Continue using the current Patient Consent Form

| | CPMS | CPMS 2.0 | |
|---|---|---|---|
| 1 | I CONSENT to my de-identified data being shared in ERN(s) for my CARE. I understand that my data will be shared with healthcare professionals in the ERN(s) so that they may work together to support my care. | I consent to my pseudonymised data being shared for my diagnosis and treatment. I am aware that my data may be shared with healthcare professionals in other hospitals, in some cases in other EU countries, so that they can discuss my case and advise my treating doctors. | ✓ |
| 2 | I CONSENT to my de-identified data being included in one or more ERN database or registry. | I consent to my clinical case being fully anonymised and then used for educational purposes. | ✘ |
| 3 | I WOULD LIKE TO BE CONTACTED about research. I will decide if I consent to my data being used for a specific project if I am contacted. | I consent to my pseudonymised clinical data being exported to ERN registries for the purpose of scientific research. | ✘ |

- The 1st consent of the current CPMS form is still valid
- The 2nd and 3rd are outdated (but are anyway optional)

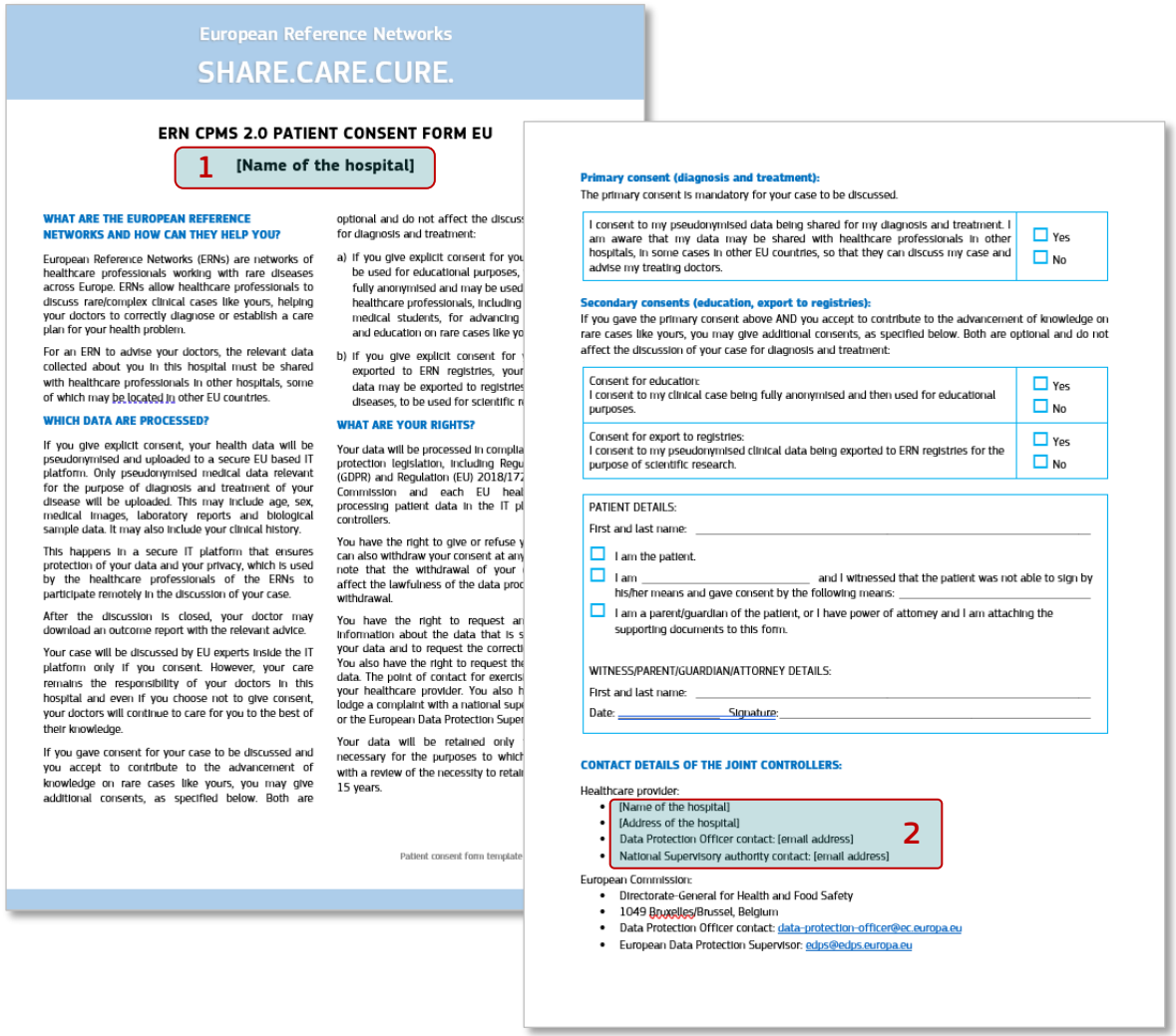
Form can still be used until an update is issued by the HCP

# Adapt the CPMS 2.0 EC recommended template kit

PREFERRED OPTION

- GDPR compliant
  - Collects consent to share personal data for specific purposes
  - Fully aligned with the processing of personal data by the CPMS 2.0
- HCPs should follow recommendations of national authorities
  - Guidelines of the national supervisory authority
  - Guidance of the national health authority, if any
    - Local initiative of the hospital
    - Centralised approach led by the national health authorities

# The CPMS 2.0 EC recommended template kit



European Reference Networks

SHARE.CARE.CURE.

**ERN CPMS 2.0 PATIENT CONSENT FORM EU**

1 [Name of the hospital]

**WHAT ARE THE EUROPEAN REFERENCE NETWORKS AND HOW CAN THEY HELP YOU?**

European Reference Networks (ERNs) are networks of healthcare professionals working with rare diseases across Europe. ERNs allow healthcare professionals to discuss rare/complex clinical cases like yours, helping your doctors to correctly diagnose or establish a care plan for your health problem.

For an ERN to advise your doctors, the relevant data collected about you in this hospital must be shared with healthcare professionals in other hospitals, some of which may be located in other EU countries.

**WHICH DATA ARE PROCESSED?**

If you give explicit consent, your health data will be pseudonymised and uploaded to a secure EU based IT platform. Only pseudonymised medical data relevant for the purpose of diagnosis and treatment of your disease will be uploaded. This may include age, sex, medical images, laboratory reports and biological sample data. It may also include your clinical history.

This happens in a secure IT platform that ensures protection of your data and your privacy, which is used by the healthcare professionals of the ERNs to participate remotely in the discussion of your case.

After the discussion is closed, your doctor may download an outcome report with the relevant advice.

Your case will be discussed by EU experts inside the IT platform only if you consent. However, your care remains the responsibility of your doctors in this hospital and even if you choose not to give consent, your doctors will continue to care for you to the best of their knowledge.

If you gave consent for your case to be discussed and you accept to contribute to the advancement of knowledge on rare cases like yours, you may give additional consents, as specified below. Both are optional and do not affect the discuss for diagnosis and treatment:

a) If you give explicit consent for you be used for educational purposes, fully anonymised and may be used healthcare professionals, including medical students, for advancing and education on rare cases like yo

b) If you give explicit consent for exported to ERN registries, your data may be exported to registries diseases, to be used for scientific r

**WHAT ARE YOUR RIGHTS?**

Your data will be processed in compli protection legislation, including Regu (GDPR) and Regulation (EU) 2018/17 Commission and each EU heal processing patient data in the IT pl controllers.

You have the right to give or refuse y can also withdraw your consent at an note that the withdrawal of your affect the lawfulness of the data proc withdrawal.

You have the right to request ar information about the data that is s your data and to request the correcti You also have the right to request the data. The point of contact for exercis your healthcare provider. You also h lodge a complaint with a national sup or the European Data Protection Super

Your data will be retained only necessary for the purposes to which with a review of the necessity to retai 15 years.

Patient consent form template

**Primary consent (diagnosis and treatment):**

The primary consent is mandatory for your case to be discussed.

| | |
|---|---|
| I consent to my pseudonymised data being shared for my diagnosis and treatment. I am aware that my data may be shared with healthcare professionals in other hospitals, in some cases in other EU countries, so that they can discuss my case and advise my treating doctors. | ☐ Yes ☐ No |

**Secondary consents (education, export to registries):**

If you gave the primary consent above AND you accept to contribute to the advancement of knowledge on rare cases like yours, you may give additional consents, as specified below. Both are optional and do not affect the discussion of your case for diagnosis and treatment:

| | |
|---|---|
| Consent for education:<br>I consent to my clinical case being fully anonymised and then used for educational purposes. | ☐ Yes ☐ No |
| Consent for export to registries:<br>I consent to my pseudonymised clinical data being exported to ERN registries for the purpose of scientific research. | ☐ Yes ☐ No |

PATIENT DETAILS:

First and last name: _____

☐ I am the patient.

☐ I am _____ and I witnessed that the patient was not able to sign by his/her means and gave consent by the following means: _____

☐ I am a parent/guardian of the patient, or I have power of attorney and I am attaching the supporting documents to this form.

WITNESS/PARENT/GUARDIAN/ATTORNEY DETAILS:

First and last name: _____

Date: _____ Signature: _____

**CONTACT DETAILS OF THE JOINT CONTROLLERS:**

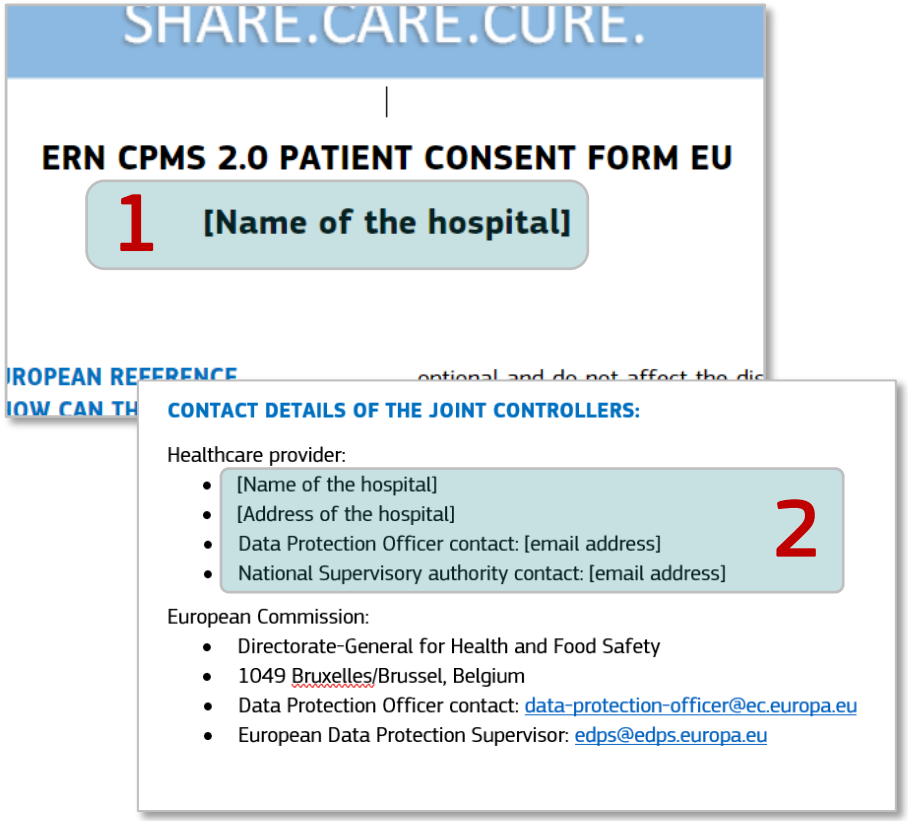
Healthcare provider:

- [Name of the hospital]
- [Address of the hospital]
- Data Protection Officer contact: [email address]
- National Supervisory authority contact: [email address]

2

European Commission:

- Directorate-General for Health and Food Safety
- 1049 Bruxelles/Brussel, Belgium
- Data Protection Officer contact: data-protection-officer@ec.europa.eu
- European Data Protection Supervisor: edps@edps.europa.eu



SHARE.CARE.CURE.

**ERN CPMS 2.0 PATIENT CONSENT FORM EU**

1 [Name of the hospital]

**CONTACT DETAILS OF THE JOINT CONTROLLERS:**

Healthcare provider:

- [Name of the hospital]
- [Address of the hospital]
- Data Protection Officer contact: [email address]
- National Supervisory authority contact: [email address]

2

European Commission:

- Directorate-General for Health and Food Safety
- 1049 Bruxelles/Brussel, Belgium
- Data Protection Officer contact: data-protection-officer@ec.europa.eu
- European Data Protection Supervisor: edps@edps.europa.eu



European Commission

# Use a different patient consent form

- Decision of the HCP
- Accountable to the national supervisory authority
- Should follow recommendations of national authorities:
  - Guidelines of the national supervisory authority
  - Guidance of the national health authority, if any
    - Local initiative of the hospital
    - Centralised approach led by the national health authorities

# DPIA of the activities under HCP responsibility

1. Already have a DPIA for the HCP activities within the current CPMS
   - If changes in the activities – assess the need of revising the DPIA

     If deemed necessary – revise it, following the guidelines of the national supervisory authority

2. Never did a DPIA for the HCP activities within the current CPMS
   - Assess the need of a DPIA

     If deemed necessary – do it, following the guidelines of the national supervisory authority

# Thank you!



European Commission