

# Data protection and privacy aspects of trust services in the context of the European Union Digital Identity Wallet

11<sup>th</sup> Trust Services and eID Forum

Alicia FILIPIAK – Commission Nationale de  
l'Informatique et des Libertés (CNIL)

# A PRIVACY TYPOLOGY OF EIDAS 2.0 PROVISIONS

## Article 5a, paragraph 4.(c)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

## Article 5a, paragraph 4.(d)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard (...)

## Article 5a, paragraph 5.(a)(x)

European Digital Identity Wallets shall, in particular: support common protocols and interfaces: (...) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

# A PRIVACY TYPOLOGY OF EIDAS 2.0 PROVISIONS

## Article 5a, paragraph 4.(c)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

- › Provisions with exclusively functional or security requirements.
- › eIDAS conformity does not impede GDPR conformity.
- › Such provisions can even ensure compliance with Articles 25 and 32 of the GDPR.

## Article 5a, paragraph 4.(d)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard (...)

- › Provisions that can be related to doctrinal work (recommendations from DPAs, guidelines from EDPB...).
- › No critical or complex impact on data protection and privacy principles.
- › However, technical implementations shall be carefully reviewed by Data Protection Authorities.

## Article 5a, paragraph 5.(a)(x)

European Digital Identity Wallets shall, in particular: support common protocols and interfaces: (...) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

- › Provisions that explicitly reference GDPR principles or Data Protection Authorities.
- › Critical impact on Data Protection measures and mitigations.
- › Critical impact on legal certainty for relevant actors of the ecosystem.

# A PRIVACY TYPOLOGY OF EIDAS 2.0 PROVISIONS

## Article 5a, paragraph 4.(c)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

- › Provisions with exclusively functional or security requirements.
- › eIDAS conformity does not impede GDPR conformity.
- › Such provisions can even ensure compliance with Articles 25 and 32 of the GDPR.

NO/LOW RISK OF MISALIGNMENT

## Article 5a, paragraph 4.(d)

European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (...) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard (...)

- › Provisions that can be related to doctrinal work (recommendations from DPAs, guidelines from EDPB...).
- › No critical or complex impact on data protection and privacy principles.
- › However, technical implementations shall be carefully reviewed by Data Protection Authorities.

INTERSECTIONS WITH DPA PRACTICES

## Article 5a, paragraph 5.(a)(x)

European Digital Identity Wallets shall, in particular: support common protocols and interfaces: (...) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

- › Provisions that explicitly reference GDPR principles or Data Protection Authorities.
- › Critical impact on Data Protection measures and mitigations.
- › Critical impact on legal certainty for relevant actors of the ecosystem.

GDPR OR DPA EXPLICIT REFERENCES

# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.

# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.

A RISK OF LEGAL MISALIGNMENT

# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.
- › Wallet providers, relying parties and other services need a clear and stabilized framework.
- › Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

A RISK OF LEGAL MISALIGNMENT

# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.
- › Wallet providers, relying parties and other services need a clear and stabilized framework.
- › Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

A RISK OF LEGAL MISALIGNMENT

A RISK OF LACK OF LEGAL CERTAINTY



# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.
- › Wallet providers, relying parties and other services need a clear and stabilized framework.
- › Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

## A RISK OF LEGAL MISALIGNMENT

- › Wallet providers frame the functionalities and capacities of wallet instances. However, they may neither be controllers nor processors under GDPR.
- › Without strong privacy considerations in the certification schemes design, Data Protection Authorities may encounter difficulties to enforce GDPR.

## A RISK OF LACK OF LEGAL CERTAINTY

# INTERPRETING AND ENFORCING EIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.
- › Wallet providers, relying parties and other services need a clear and stabilized framework.
- › Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

## A RISK OF LEGAL MISALIGNMENT

- › **Wallet providers frame the functionalities and capacities of wallet instances. However, they may neither be controllers nor processors under GDPR.**
- › **Without strong privacy considerations in the certification schemes design, Data Protection Authorities may encounter difficulties to enforce GDPR.**

## A RISK OF LACK OF LEGAL CERTAINTY

## SOME DEAD ANGLES FOR DATA PROTECTION

# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.

## A RISK OF LEGAL MISALIGNMENT

- › Wallet providers frame the functionalities and capacities of wallet instances. However, they may neither be controllers nor processors under GDPR.
- › Without strong privacy considerations in the certification schemes design, Data Protection Authorities may encounter difficulties to enforce **GDPR**.

## SOME DEAD ANGLES FOR DATA PROTECTION

- › Wallet providers, relying parties and other services need a clear and stabilized framework.
- › Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

## A RISK OF LACK OF LEGAL CERTAINTY

- › **Privacy Enhancing Technologies can lack the maturity or the industrial incentive for strong certification guarantees in standardization bodies.**
- › **However, for some use cases that do not require strong security, such as Age Verification, they can be relevant and shall be promoted.**

# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.

## A RISK OF LEGAL MISALIGNMENT

- › Wallet providers frame the functionalities and capacities of wallet instances. However, they may neither be controllers nor processors under GDPR.
- › Without strong privacy considerations in the certification schemes design, Data Protection Authorities may encounter difficulties to enforce **GDPR**.

## SOME DEAD ANGLES FOR DATA PROTECTION

- › Wallet providers, relying parties and other services need a clear and stabilized framework.
- › Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

## A RISK OF LACK OF LEGAL CERTAINTY

- › **Privacy Enhancing Technologies can lack the maturity or the industrial incentive for strong certification guarantees in standardization bodies.**
- › **However, for some use cases that do not require strong security, such as Age Verification, they can be relevant and shall be promoted.**

## A DELICATE BALANCE BETWEEN SECURITY AND PRIVACY

# INTERPRETING AND ENFORCING eIDAS 2.0

- › The eIDAS 2.0 Regulation defines new roles for National and European administrations.
- › With no cohesive and coordinated cooperation between said administrations, the Regulation's provisions can be interpreted differently.

## A RISK OF LEGAL MISALIGNMENT

- › Wallet providers frame the functionalities and capacities of wallet instances. However, they may neither be controllers nor processors under GDPR.
- › Without strong privacy considerations in the certification schemes design, Data Protection Authorities may encounter difficulties to enforce **GDPR**.

## SOME DEAD ANGLES FOR DATA PROTECTION

- › Wallet providers, relying parties and other services need a clear and stabilized framework.
- › Transparency and guarantees for the user to have control over their personal data are critical for the wide adoption of trust services and eID solutions.

## A RISK OF LACK OF LEGAL CERTAINTY

- › Privacy Enhancing Technologies can lack the maturity or the industrial incentive for strong certification guarantees in standardization bodies.
- › However, for some use cases that do not require strong security, such as Age Verification, they can be relevant and shall be promoted.

## A DELICATE BALANCE BETWEEN SECURITY AND PRIVACY

# THE FRENCH TOUCH

# THE FRENCH TOUCH

**THE FRENCH  
ADMINISTRATIONS CHOSE  
TO INCLUDE ITS DPA – THE  
CNIL – IN THE FRENCH  
EIDAS EXPERT GROUP**

# THE FRENCH TOUCH

**THE FRENCH  
ADMINISTRATIONS CHOSE  
TO INCLUDE ITS DPA – THE  
CNIL – IN THE FRENCH  
EIDAS EXPERT GROUP**

**DIGITAL IDENTITY IS NOW  
AT THE HIGHEST LEVEL IN  
THE CNIL'S STRATEGIC  
PLAN FOR 2025-2028**



# THE FRENCH TOUCH

**THE FRENCH ADMINISTRATIONS CHOSE TO INCLUDE ITS DPA – THE CNIL – IN THE FRENCH EIDAS EXPERT GROUP**

**DIGITAL IDENTITY IS NOW AT THE HIGHEST LEVEL IN THE CNIL'S STRATEGIC PLAN FOR 2025-2028**

**THE EDPB WAS INCLUDED AS AN OBSERVER IN THE EUROPEAN DIGITAL IDENTITY COOPERATION GROUP AT THE CNIL'S AND THE FRENCH EIDAS EXPERT GROUP'S INITIATIVE**

# POSSIBLE SYNERGIES AND ACTIONS

# POSSIBLE SYNERGIES AND ACTIONS

PROMOTE AND  
PROTECT DATA  
PROTECTION  
PRINCIPLES IN THE  
EIDAS LEGAL  
FRAMEWORK

# POSSIBLE SYNERGIES AND ACTIONS

PROMOTE AND  
PROTECT DATA  
PROTECTION  
PRINCIPLES IN THE  
EIDAS LEGAL  
FRAMEWORK

IDENTIFY DATA  
PROTECTION AND  
PRIVACY ASPECTS  
IN THE WIDE  
TRUST SERVICES  
AND EID  
ECOSYSTEM SUCH  
AS THE EUDIW BUT  
ALSO THE AGE  
VERIFICATION  
APPLICATIONS  
AND OTHER LARGE  
SCALE PILOTS  
PROPOSALS

# POSSIBLE SYNERGIES AND ACTIONS

PROMOTE AND  
PROTECT DATA  
PROTECTION  
PRINCIPLES IN THE  
EIDAS LEGAL  
FRAMEWORK

IDENTIFY DATA  
PROTECTION AND  
PRIVACY ASPECTS  
IN THE WIDE  
TRUST SERVICES  
AND EID  
ECOSYSTEM SUCH  
AS THE EUDIW BUT  
ALSO THE AGE  
VERIFICATION  
APPLICATIONS  
AND OTHER LARGE  
SCALE PILOTS  
PROPOSALS

KEEP IN MIND  
THAT THE EDPB IS  
WORKING ON  
GDPR  
CERTIFICATIONS  
FOCUSED ON  
DIGITAL IDENTITY  
ASPECTS

# POSSIBLE SYNERGIES AND ACTIONS

**PROMOTE AND  
PROTECT DATA  
PROTECTION  
PRINCIPLES IN THE  
EIDAS LEGAL  
FRAMEWORK**

**IDENTIFY DATA  
PROTECTION AND  
PRIVACY ASPECTS  
IN THE WIDE  
TRUST SERVICES  
AND EID  
ECOSYSTEM SUCH  
AS THE EUDIW BUT  
ALSO THE AGE  
VERIFICATION  
APPLICATIONS  
AND OTHER LARGE  
SCALE PILOTS  
PROPOSALS**

**KEEP IN MIND  
THAT THE EDPB IS  
WORKING ON  
GDPR  
CERTIFICATIONS  
FOCUSED ON  
DIGITAL IDENTITY  
ASPECTS**

**INCLUDE DATA  
PROTECTION  
AUTHORITIES AT  
NATIONAL AND  
EUROPEAN LEVELS!**

# Thank you for your attention!

Any questions?