

THE PRIVACY, THE SECRECY AND THE CONTRADICTION OF NIS 2 FRAMEWORK

RODRIGO PANCHINIAK FERNANDES

PROGRAMMER, AUTHOR AND MAINTAINER OF **PROTECTED CONTENT**, AN OPEN
SOURCE END-TO-END, CLIENT SIDE, ZERO TRUST ENCRYPTION MODULE THAT
IMPLEMENTS THE GREAT OPENPGPJS

NETWORK AND INFORMATION SECURITY

WHAT IS 2 IN NIS 2 AND WHY IT
SHOULD NOT BE THERE?

WHEN WE DO NOT WANT SECRECY TO
WIN?...

ACCUEIL • SOCIÉTÉ • RÉGIONS • WALLONIE

Un éducateur dans une école maternelle arrêté pour pédopornographie

A Liège, à l'école du Sart Liman, les parents des 400 élèves de l'école maternelle et primaire ont reçu une lettre annonçant l'arrestation d'un éducateur en raison de la découverte de matériel pédopornographique à son domicile.



RECITAL (95)

IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.

~~IN ORDER~~ TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC~~ COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES,~~ THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES,~~ THE USE OF ~~ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS,~~ SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

~~IN ORDER TO SAFEGUARD THE SECURITY OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES, THE USE OF ENCRYPTION TECHNOLOGIES, IN PARTICULAR END-TO-END ENCRYPTION AS WELL AS DATA-CENTRIC SECURITY CONCEPTS, SUCH AS CARTOGRAPHY, SEGMENTATION, TAGGING, ACCESS POLICY AND ACCESS MANAGEMENT, AND AUTOMATED ACCESS DECISIONS, SHOULD BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

TO SAFEGUARD THE SECURITY OF

COMMUNICATIONS

THE USE

OF

END-TO-END ENCRYPTION

SHOULD

BE PROMOTED. WHERE NECESSARY, THE USE OF ENCRYPTION, IN PARTICULAR END-TO-END ENCRYPTION SHOULD BE MANDATORY FOR PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES IN ACCORDANCE WITH THE PRINCIPLES OF SECURITY AND PRIVACY BY DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.

TO SAFEGUARD THE SECURITY OF

COMMUNICATIONS

THE USE

OF

END-TO-END ENCRYPTION

SHOULD

BE PROMOTED.

END-TO-

END ENCRYPTION SHOULD BE MANDATORY FOR

COMMUNICATIONS

BY

~~DEFAULT AND BY DESIGN FOR THE PURPOSES OF THIS DIRECTIVE. THE USE OF END-TO-END ENCRYPTION SHOULD BE RECONCILED WITH THE MEMBER STATES' POWERS TO ENSURE THE PROTECTION OF THEIR ESSENTIAL SECURITY INTERESTS AND PUBLIC SECURITY, AND TO ALLOW FOR THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER, THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE SECURITY OF COMMUNICATIONS.~~

TO SAFEGUARD THE SECURITY OF
OF COMMUNICATIONS
END-TO-END ENCRYPTION
THE USE
SHOULD
END-TO-
BE PROMOTED.
END ENCRYPTION SHOULD BE MANDATORY FOR
COMMUNICATIONS
BY
END-
DEFAULT AND BY DESIGN
TO-END ENCRYPTION SHOULD

ALLOW FOR THE DETECTION
OF CRIMINAL OFFENCES IN ACCORDANCE WITH UNION LAW. HOWEVER,
THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION, WHICH IS A CRITICAL
TECHNOLOGY FOR THE EFFECTIVE PROTECTION OF DATA AND PRIVACY AND THE
SECURITY OF COMMUNICATIONS.

TO SAFEGUARD THE SECURITY OF
OF
END-TO-END ENCRYPTION
COMMUNICATIONS
THE USE
SHOULD
END-TO-
END ENCRYPTION SHOULD BE MANDATORY FOR
COMMUNICATIONS
BY
END-
DEFAULT AND BY DESIGN
TO-END ENCRYPTION SHOULD
ALLOW FOR THE
OF CRIMINAL OFFENCES
THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION
DETECTION
HOWEVER,

TO SAFEGUARD THE SECURITY OF
OF COMMUNICATIONS
THE USE
END-TO-END ENCRYPTION
SHOULD
BE PROMOTED.
END-TO-
END ENCRYPTION SHOULD BE MANDATORY FOR
COMMUNICATIONS
BY
END-
DEFAULT AND BY DESIGN
TO-END ENCRYPTION SHOULD
ALLOW FOR THE
OF CRIMINAL OFFENCES
DETECTION
THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION
HOWEVER,

TO SAFEGUARD THE SECURITY

END-TO-END ENCRYPTION

BE PROMOTED.

END ENCRYPTION SHOULD BE MANDATORY

DEFAULT AND BY DESIGN

TO-END ENCRYPTION SHOULD

ALLOW FOR THE

OF CRIMINAL OFFENCES

THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION

SHOULD

END-TO-

BY

END-

DETECTION

HOWEVER,

1. TO SAFEGUARD THE SECURITY

END-TO-END ENCRYPTION

BE PROMOTED.

END ENCRYPTION SHOULD BE MANDATORY

DEFAULT AND BY DESIGN

TO-END ENCRYPTION SHOULD

ALLOW FOR THE

OF CRIMINAL OFFENCES

THIS SHOULD NOT WEAKEN END-TO-END ENCRYPTION

SHOULD

2. END-TO-

BY

3. END-

DETECTION

4. HOWEVER,

1. TO SAFEGUARD THE SECURITY

END-TO-END ENCRYPTION

BE PROMOTED.

END ENCRYPTION SHOULD BE MANDATORY

DEFAULT AND BY DESIGN

TO-END ENCRYPTION SHOULD

ALLOW FOR THE

OF CRIMINAL OFFENCES

//// SHOULD NOT WEAKEN END-TO-END ENCRYPTION

SHOULD

2. END-TO-

BY

3. END-

DETECTION

4. HOWEVER,

1. TO SAFEGUARD THE SECURITY

END-TO-END ENCRYPTION

BE PROMOTED.

END ENCRYPTION SHOULD BE MANDATORY

DEFAULT AND BY DESIGN

TO-END ENCRYPTION SHOULD

ALLOW FOR THE

OF CRIMINAL OFFENCES

3 SHOULD NOT WEAKEN END-TO-END ENCRYPTION

SHOULD

2. END-TO-

BY

3. END-

DETECTION

4. HOWEVER,

1. TO SAFEGUARD THE SECURITY, END-TO-END ENCRYPTION SHOULD BE PROMOTED.
2. END-TO-END ENCRYPTION SHOULD BE MANDATORY BY DEFAULT AND BY DESIGN
3. END-TO-END ENCRYPTION SHOULD ALLOW FOR THE DETECTION OF CRIMINAL OFFENCES
4. HOWEVER, 3 SHOULD NOT WEAKEN END-TO-END ENCRYPTION

This apparent contradiction has a solution

"policy makers should refrain from measures that could weaken encryption. We strictly oppose any technical solutions, such as backdoors or master key, as their pure existence would weaken encryption in the EU. Europe needs not fewer, but more trustworthy IT solutions to swiftly implement the digital transformation in administration, industry and society. To this end, European legislators should be proponents of strong encryption."

**Federation of German Industries,
16 March 2021**

Society should not accept
that violation of
communication is
admissible

If we can not accept the
public risk of 1-to-1
communication, then we
should explicitly and
transparently define a 3rd

Not as an institution, but as a
private person active
representative of an institution

That's it!

Questions?
Comments?

