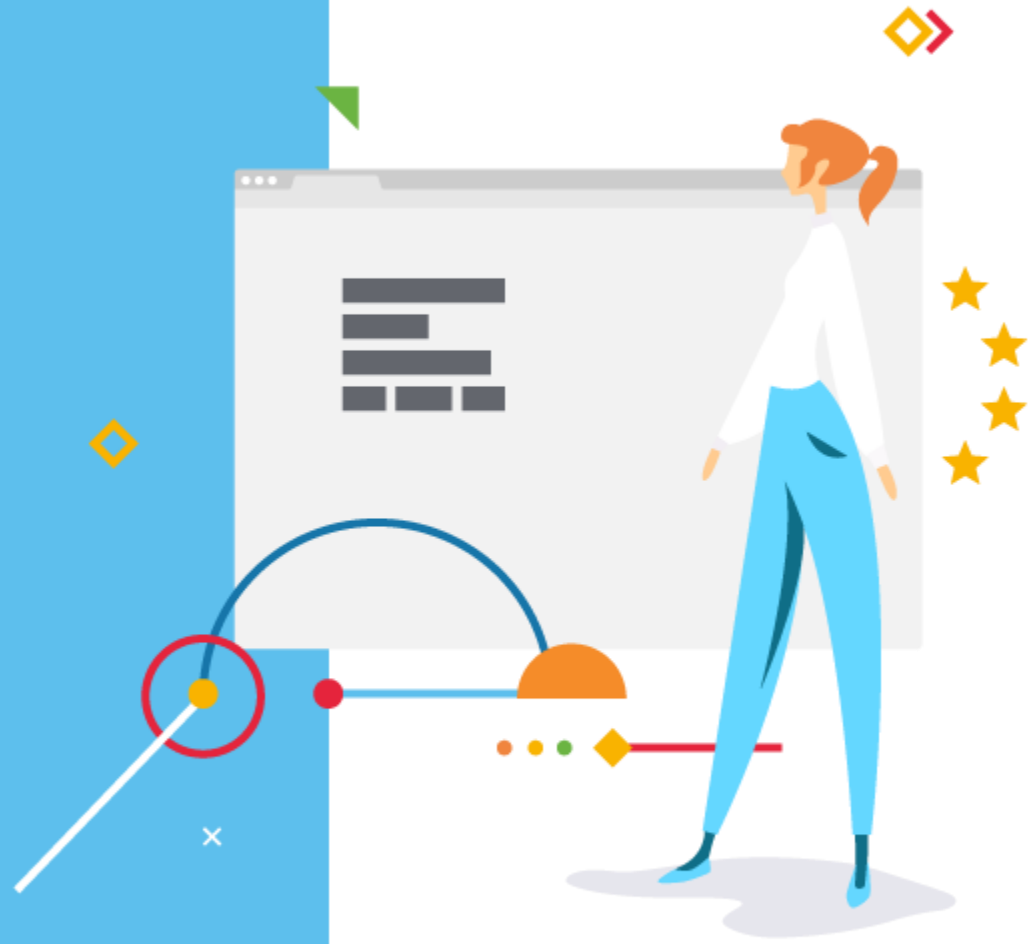
GDPR

& Enterprise Messaging



CLX MEF XConnect TeachPrivacy

TODAY'S

DISCUSSION

Introductions

Professor Daniel Solove

GDPR Expert - Teachprivacy

Rob Malcolm

VP Marketing & Online Sales CLX

Tim Green

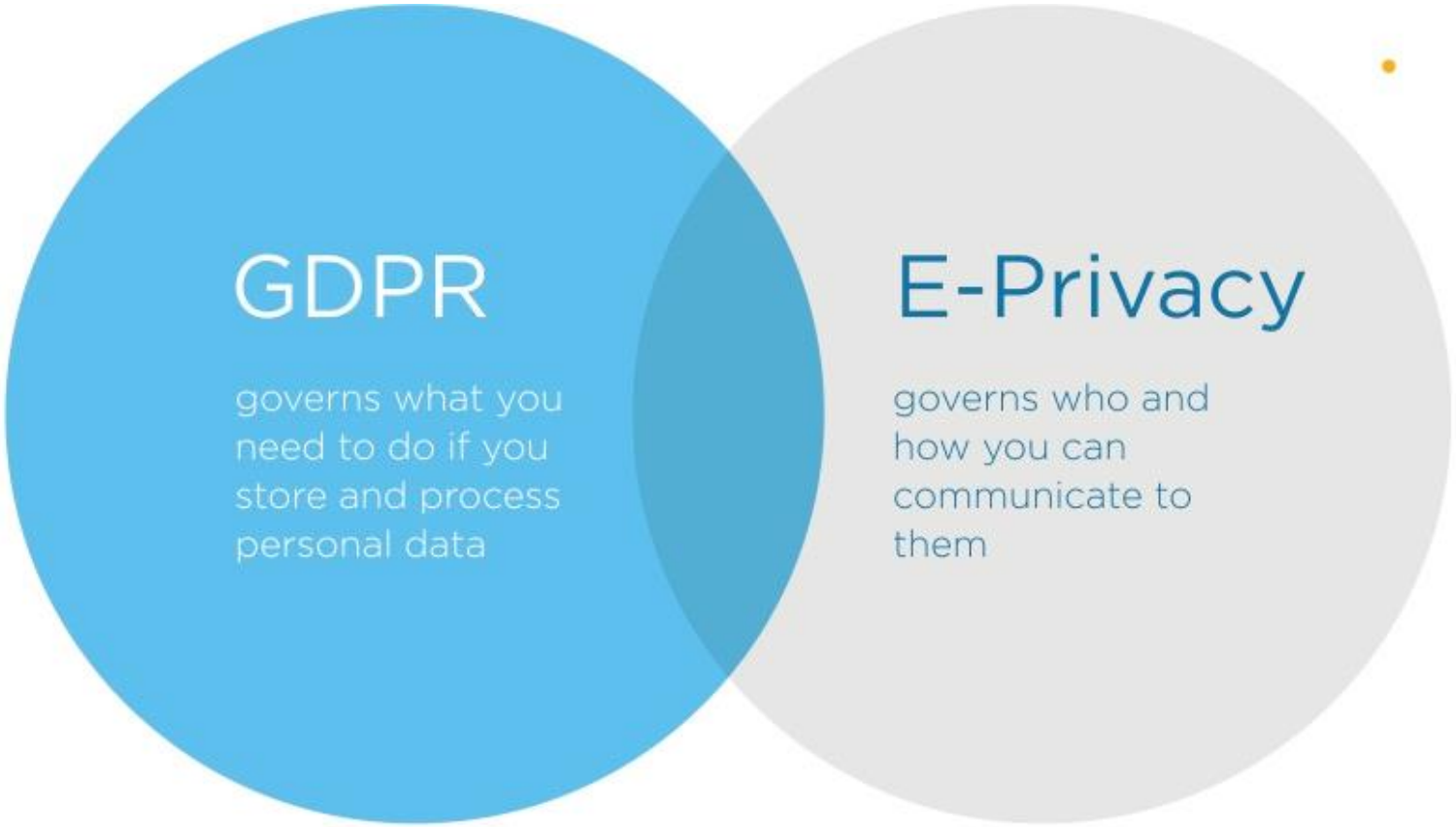
Features Editor - MEF

Lee Suker

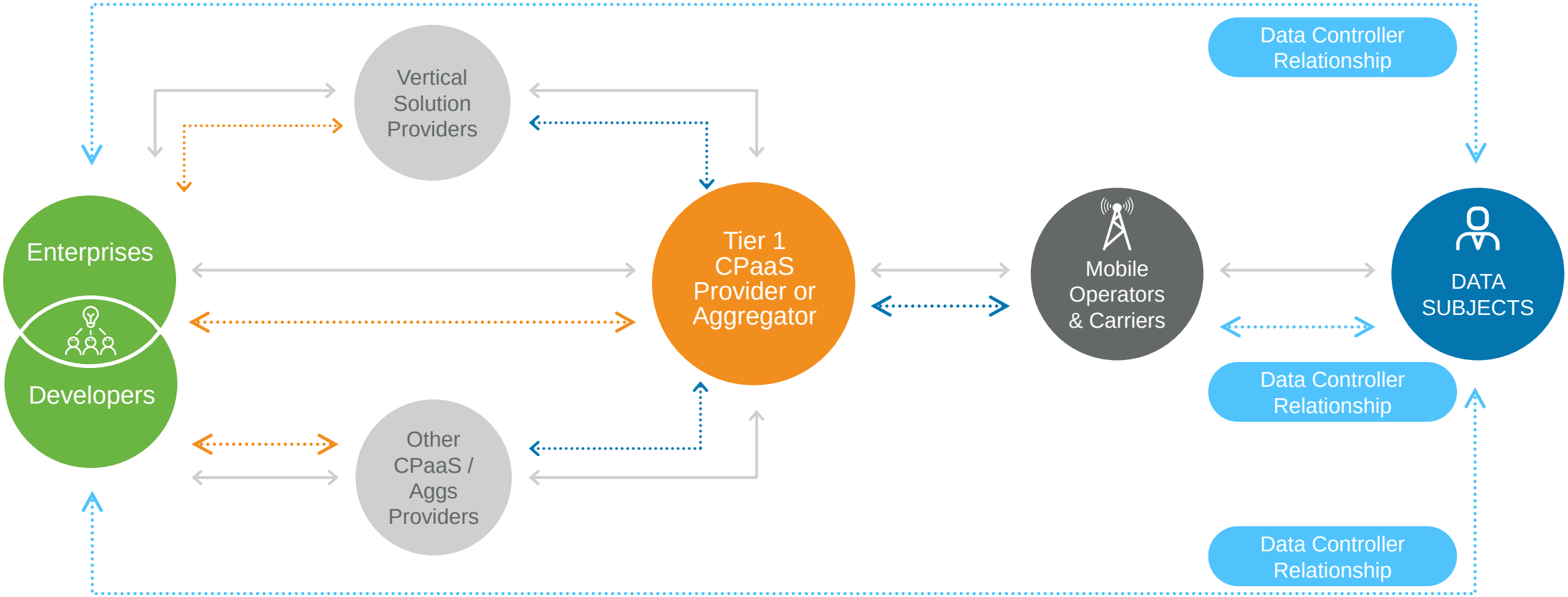
Market Development Director , DPO- XConnect

What is GDPR?

Data Privacy in the EU is covered under two regulations.



The players – for message transmission



Message Flow

Data Controller Relationship

Data Processor Relationship

Data Sub-Processor Relationship

All CPaaS Providers / Aggregators are both Data Controllers and Data Processors

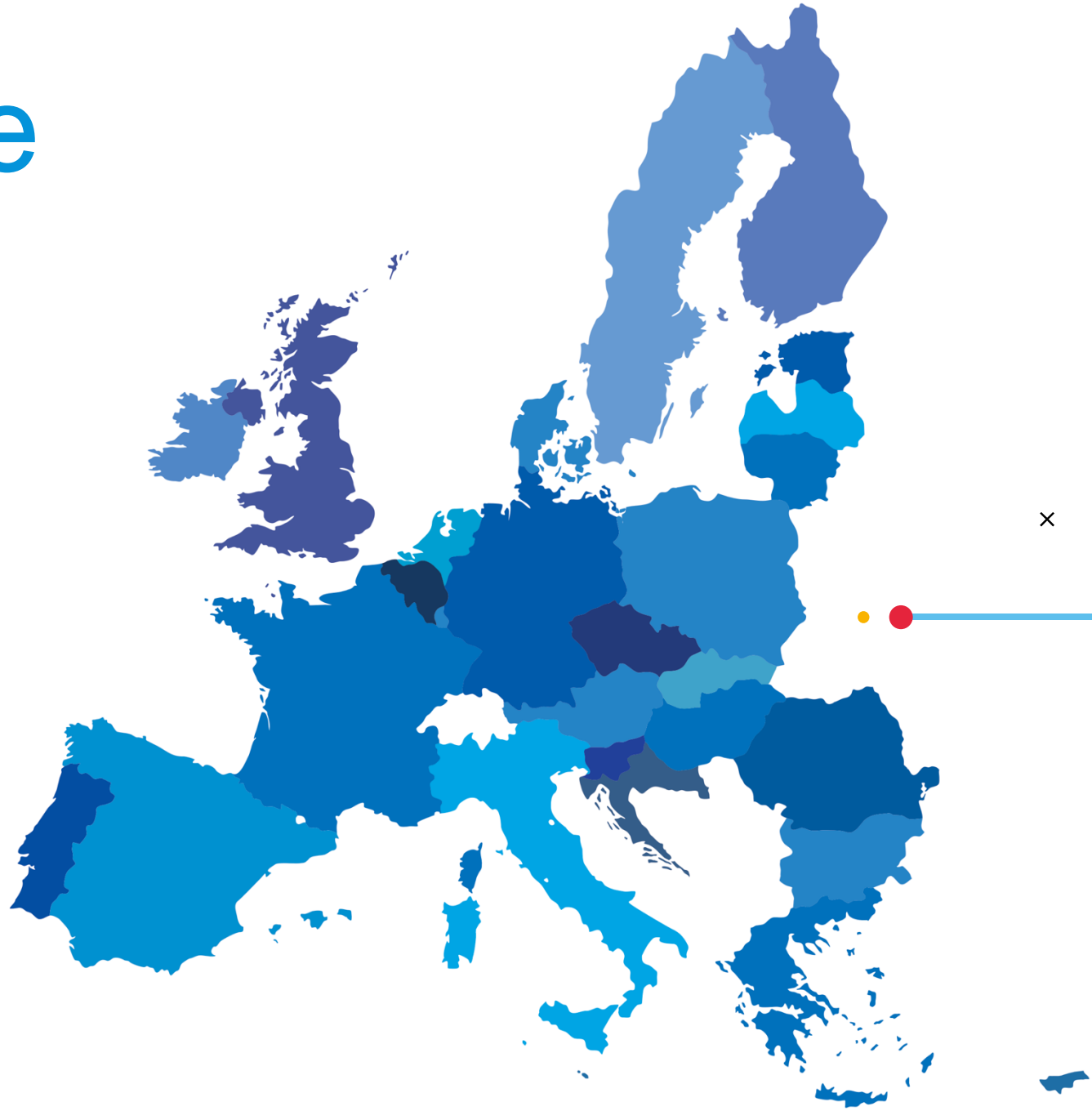
Territorial Scope

All companies based in the EU

Any company sending to or receiving a message from an EU Data Subject

Any company hosting or serving MNP (or other Personal Data) information containing EU ‘Data Subject’ information

Note that a browser accessing the data (e.g. for support) will store data



What is personal data?

In the context of messaging

Unique Addressing

- MSISDN
- IMSI
- Email Address
- OTT Address (e.g. skype address)
- IP Address

Anything within the content of a message that can uniquely identify a EU citizen e.g.

- Name
- Bank account / Credit Card number
- Drivers License
- National Insurance / ID Number
- Policy Number
- Booking Reference
- Car Registration Number
- A combination of identification elements e.g. physical characteristics, place, occupations etc.

Note that **meta data** related to communications e.g. a MSISDN combined with a destination and timestamp is still regarded as personal data

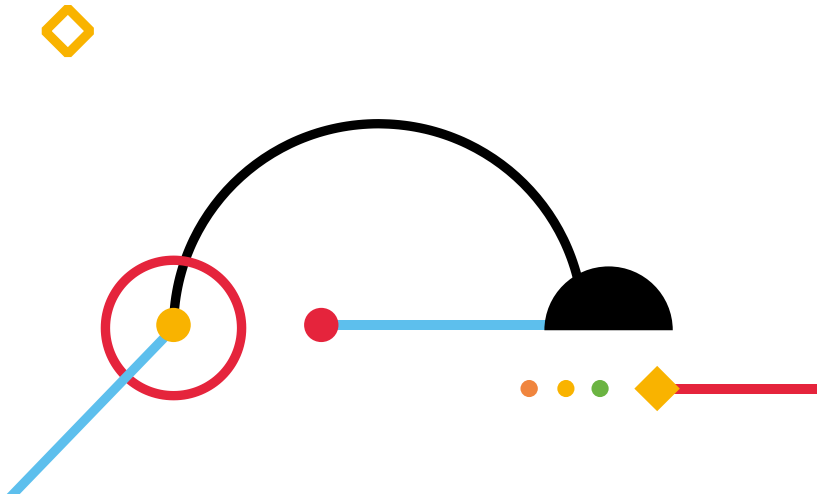
Does data need to be kept in the EU?

GDPR states that data can be stored in any country provided they have “Adequate Levels of Data Protection”

Personal Data can flow freely

- within All EEA countries
- In addition so far Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay
- USA (where entities have signed up to the Privacy Shield framework)
- Japan and South Korea are close to being approved

If Personal Data is transferred out of the EU then the legal entity handling the data in another country needs to be GDPR compliant



Do I need to get my customers to re-opt in

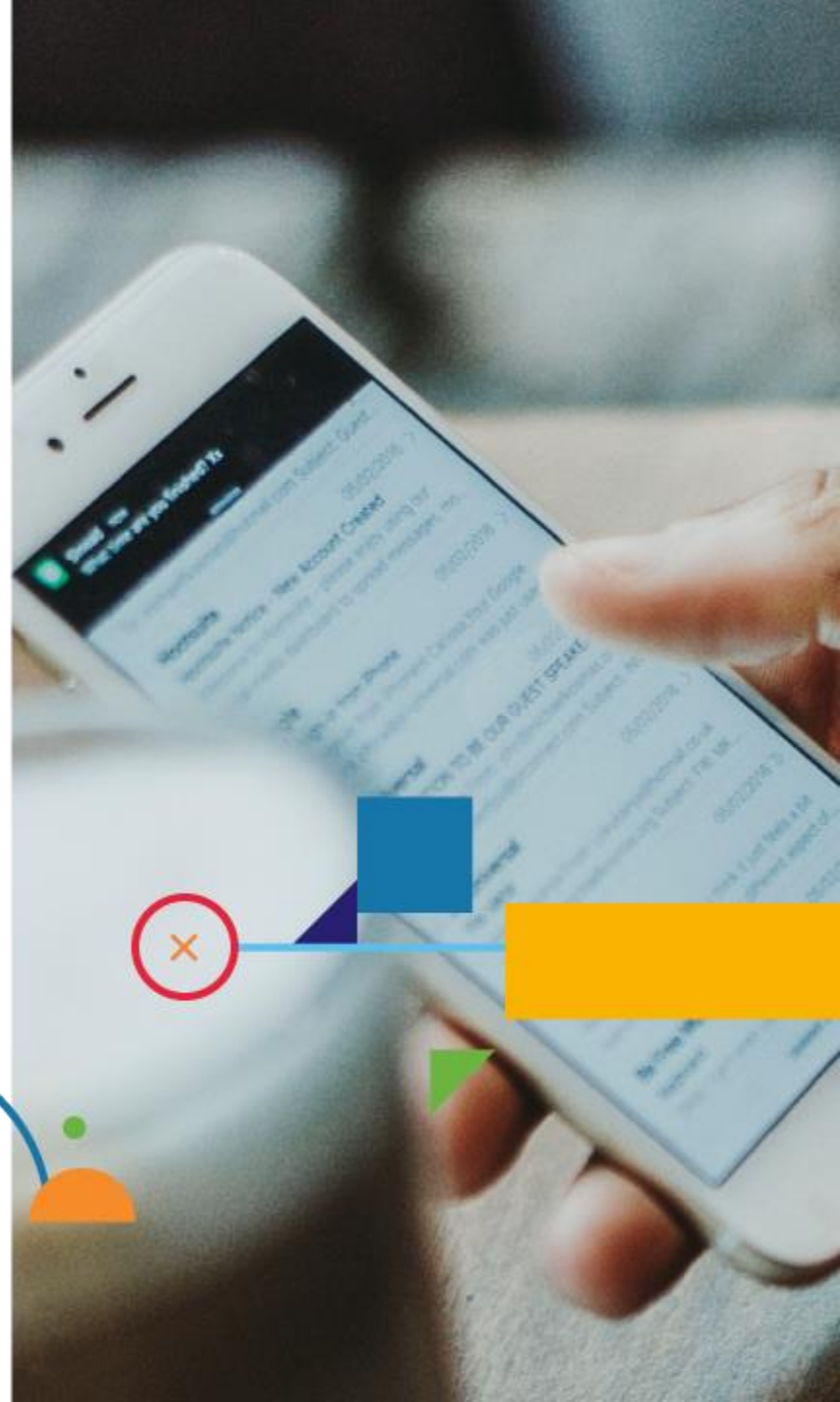
GDPR covers the consent to store and process Personal Data. This should not be confused with the consent to be communicated too.

50% of GDPR is obtaining consent to store Personal Data.

- What information will be stored
- How long will it be stored for
- How will the data be handled
- Who will have access to it
- What is the process for data to be modified or deleted

Gaining consent is almost always the responsibility of the company who owns the message recipient as a customer

If you have the consent to store Personal Data then there is not need to seek Opt-in to continue to communicate with your customer



What has CLX done to prepare?

Created processes to allow for our customers to request data to modified or deleted

Restricted the time we store log files to the absolute minimum time after which we anonymize the data

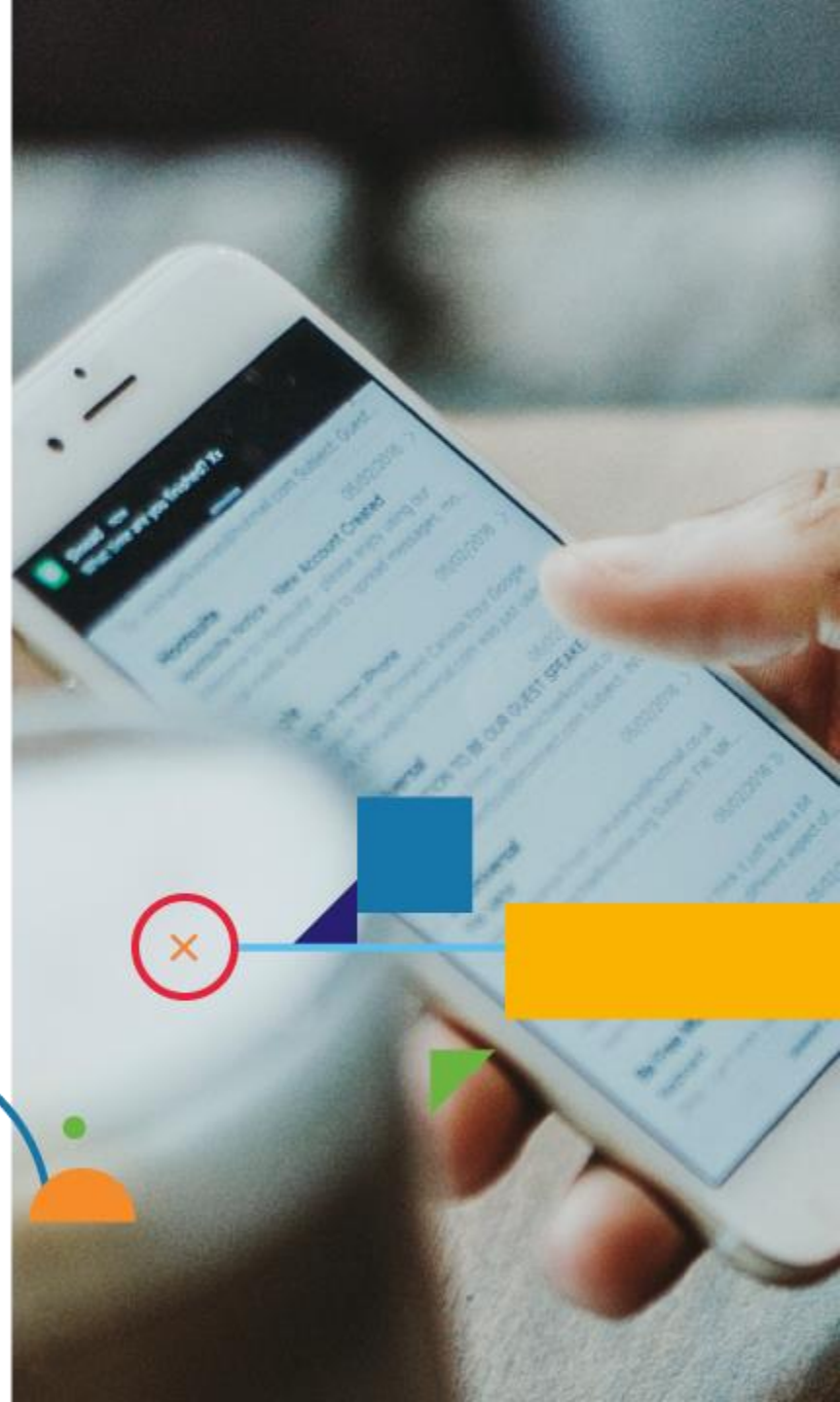
Created an EEA based infrastructure that guarantees message data will remain in the EEA if requested

Created a GDPR specific routing class that ensures messages to EU Data Subjects only uses MNO's in the EU

Created a support email address and contact that ensures all support requests are handled by teams in the EU

Trained out teams on GDPR compliance

Signing a Data Protection Agreement with all our customers, and suppliers



QUESTIONS & DISCUSSION

THANKS

For more information about MEF's Future of Messaging Programme, please contact:

messaging@mobileecosystemforum.com