



PROGRAM MATERIALS
Program #30121
April 16, 2020

Data Protection in a Pandemic: GDPR vs. COVID-19

**Copyright ©2020 by Odia Kagan, Esq. - Fox Rothschild
LLP and Peter Hense - Spirit Legal. All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

DATA PROTECTION IN AN AGE OF PANDEMIC: GDPR AND COVID-19

Odia Kagan
Chair of GDPR Compliance and International Privacy
Fox Rothschild LLP
okagan@foxrothschild.com
+1-215-444-7313
[LinkedIn](#)

Peter Hense
Head of Data Protection
Spirit Legal Rechtsanwälte
Germany
peter.hense@spiritlegal.com
[LinkedIn](#)

COVID-19



Fox Rothschild LLP
ATTORNEYS AT LAW



THE LEGAL REGIME: TO GDPR OR NOT TO GDPR?

GDPR does NOT SUSPEND fighting COVID-19

- Data protection law does not stand in the way of the provision of healthcare and the management of public health issues
- The fight against communicable diseases is a valuable goal shared by all nations and therefore, should be supported in the best possible way.

[EDPB]



GDPR does NOT SUSPEND fighting COVID-19

“It’s a balance here. How data can be used on one side to control the virus and pandemic, while still maintaining fundamental values that make our societies what they are,”

“This is a new situation, but we still have our values that have built our society... We want to come back to a society that may have changed, but not changed in a fundamental way that we still have a sense of individuality and you have rights that should not be undermined.

[EU competition chief Margarethe Vestager.]



Fox Rothschild LLP
ATTORNEYS AT LAW

GDPR does NOT SUSPEND fighting COVID-19

- Public health is paramount and prevention and the right to privacy are not incompatible [Belgium APD]
- Data protection should not be used to hinder or limit the effectiveness of the measures taken by authorities in the fight against the pandemic. [Spain AEPD]
- Data protection law does not stand in the way of the provision of healthcare or management of public health [Ireland DPC]

Data Processing should help not hurt

- Do not encourage panic by increasing half-truths and assumptions.
- Protect data so as to prevent the dissemination of unjustified and disproportionate information on specific infected persons or persons at risk.
- Unjustified processing of personal data may promote discrimination and pose a risk to the rights and freedoms of natural persons, as well as adversely affect their economic and social situation

[Latvian Datu Valsts Inspekcija]



Fox Rothschild LLP
ATTORNEYS AT LAW

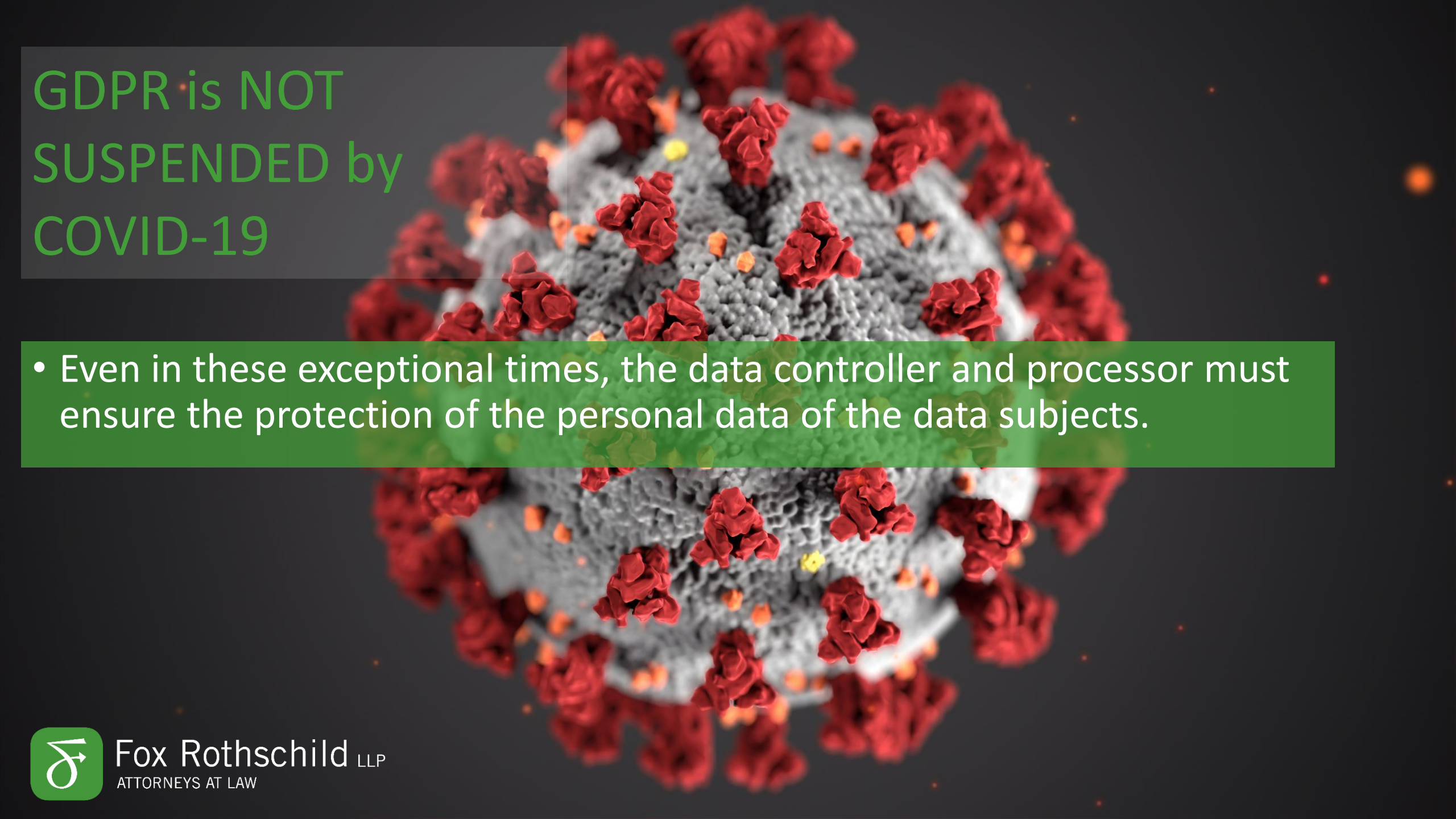
GDPR is NOT SUSPENDED by COVID-19

EDPS

"Covid-19 is a game changer ... Whatever happens in the next few weeks, we know the words will not be the same. We will all be confronted with this game changer in one way or another. And we will all ask ourselves whether we are ready to sacrifice our fundamental rights in order to feel better and to be more secure."

[EDPS]





GDPR is NOT SUSPENDED by COVID-19

- Even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects.

GDPR is NOT SUSPENDED by COVID-19

- "In times of crisis, privacy is sometimes compared to safety or public health. That is a false contradiction. We must protect both public health and our fundamental right to privacy. And always in the right balance."
- "We live in a democratic country. This also applies in times of crisis."

[Netherlands - Autoriteit Persoonsgegevens]



Emergency laws trump GDPR

- Emergency may legitimize restrictions of freedoms
- Restrictions must be necessary + proportionate.
- Subject to judicial control of the CJEU and ECHR
- Must be strictly limited to the duration of the emergency at hand.
- Controllers must comply with applicable emergency regulations





THE CORE PRINCIPLES

Types of Data

- Information that an employee has been infected with coronavirus is Health Information.
- Information that an employee has returned from a risk area is not Health Information.
- The fact that the employee is in quarantine (without giving further information for a reason) is not Health information.-
- Health records may be processed only by those persons who are in charge of them

[Finland TT, Norway Datatilsynet]



Core Principles

- Data Minimization – only collect the data necessary for the purpose.
- Transparency – provide full disclosure (Art 13/14)
- Adequate security – for disclosing COVID-19 information

Legal Basis

The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person.

[Recital 46 GDPR]

Legal Basis

Type of Entity	Legal Basis	Source / Citation	
Public Health Authorities	necessary for reasons of <u>substantial public interest in the area of public health</u> .	<ul style="list-style-type: none"> • 6.1.(e) and + 9.2.(i) - the control of epidemics and their spread, • 6+ 9.2(g) GDPR + local act on public health • 6.1.(d) - vital interests of an individual or all susceptible to be infected 	suitable <u>safeguards</u> (e.g access limitation, strict time limits for erasure, adequate staff training, pseudonymization, encryption, appointing DPO [e.g. sec. 22 BDSG, Germany])
Employers	compliance with a legal obligation	employer's prevention of occupational risks for personnel).	
		Consent?	



LOCATION DATA



Fox Rothschild ^{LLP}
ATTORNEYS AT LAW

Communications

- Public health messages are not direct marketing. [UK ICO]

Location Data

- If at all possible – should be made anonymous.
 - Can it be made anonymous?
- The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved



Location Data

- Identified location data permitted under Member State law to safeguard public security
 - Must be Necessary + appropriate + proportionate + judicial recourse
- Surveillance and monitoring measures should be written in law and clearly limited in time. [UN]
- Governments should also favor voluntary tools such as phone-tracking app requiring users' consent over broader surveillance power [UN]



EMPLOYERS

Employers (1)

- COLLECT- health data only if permitted by law
- PROCESS - health data only if legally required (employment or health laws)
- INFORM - staff about COVID-19 cases and take protective measures

Employers (2)

- DON'T - collect information in a systematic, constant and generalized manner i.e no general questionnaires [**Hellenic DPA**]
- DON'T - request/collect information on the presence or absence of any flu symptoms or travel of the worker and his closest contacts
- DON'T - collect temperature at the entrance [**e.g. Germany**]



Employers (3)

- DON'T - communicate more information than necessary. [CNIL]
- DON'T - disclose that an employee has the virus to their colleagues. [CNIL]
- DON'T - disclose who died, if that leads to the identification of living persons [Hellenic DPA]
- DON'T - disclose data if that may lead to stigmas and prejudice [Hellenic DPA]
- RETAIN - only minimum information necessary (for wage/collective agreement) [Iceland]

Employers (4)

- DO - give employees information about the disease and steps to take
- DO – give employees applicable travel warnings
- DO - invite employees to report conditions where applicable
- DO- facilitate the procedures for making the reports;
- DO - advise staff to call emergency services if experiencing symptoms



Employers (5)

- DO - educate and invite employees to self check
- DO - promote remote working methods and encourage the use of occupational medicine
- DO – Implement clear procedures on self-isolation in case of contagion



Employers (6)

- MUST - Develop a pandemic/business continuity action plan
- MUST - Draft and distribute to employees an information document
- MAY - Limit unnecessary travel
- MAY - Instruct employees to self report any contact with anyone who has tested positive.

[Hungary]

Employers (7)

- MAY- ask people to tell you if they have visited a particular country, or are experiencing COVID-19 symptoms
- MAY - ask visitors to consider government advice before they decide to come.



Employers (8)

CONSIDER:

- Is there a good reason to record or disclose the information?
- Is it necessary to specify the information, -- can the purpose be achieved by "telling less"
- Is it necessary to name the person infected and / or in the home quarantine
- Can you just say "illness" and not "COVID-19"?



Employers (9)

- MAY - collect the personal contact information of employees for purpose of efficient communication [Austrian AT]
- MAY NOT - use the information for any other purpose [Austrian AT]
- MUST - delete the information after the pandemic is over. [Austrian AT]
- MUST - provide a full disclosure of this (Art 13/14) [Austrian AT]
- MUST - implement adequate protections [Iceland]



Employers (10)

CONSIDER stopping use of biometric identifiers:

“Managers should refrain from collecting or processing data biometric using physical, electronic fingerprints, or any other mechanism that allow the spread of the coronavirus through indirect contact.

This instruction does not apply in the case of biometric identification systems in that the device is for personal and individual use.”

[Colombia Superintendency of Industry and Commerce]

•

Employers (11)

If an employee reports an illness you may record:

- The date and identity of the person; [**CNIL, Netherlands, Hungary**]
- Telephone number and address [**Netherlands, Hungary**]
- Private number only with consent [**Germany**]
- How long employee thinks illness will last [**Netherlands**]

Employers (12)

- Current activities and arrangements [**Netherlands**]
- Whether illness is related to an accident at work [**Netherlands**]
- The organizational measures taken (confinement, teleworking, orientation and contact with the occupational doctor, etc.) [**CNIL**]
- The fact of whether or not the destination and dates or the employee's foreign travel (business or personal) is to locations deemed high risk [**Hungary**]



ENFORCEMENT ALLOWANCE

Enforcement allowance

"acknowledges the significant impact of the Covid-19 health crisis which may affect organisations' ability to action GDPR requests from individuals, such as access requests. [DPC]"

"understands that the current situation creates many challenges for institutions." [Canada OIC]

Enforcement allowance

The Commissioner

- Is deeply conscious of the impact that the coronavirus is having on health bodies in particular and that the prioritization of patient care may mean the diversion of resources.
- Is also conscious that some businesses will be closed all together for, what may be, a significant period.
- Will as far as possible, take a proportionate and pragmatic regulatory approach.

[Isle of Man]

Enforcement allowance

“While the statutory obligations cannot be waived, should a complaint be made to the DPC, the facts of each case including any organization specific extenuating circumstances will be fully taken into account”. [DPC]

“We are committed to being as flexible as Netherlands possible with our investigation timelines. Institutions must take all reasonable measures to limit the impact on individuals’ right of access to information” [Canada OIC]

Enforcement allowance

“This is not the time for strict enforcement of data protection. We are showing agility during this crisis”. [Norway Datatilsynet]

The ICO is a reasonable and pragmatic regulator... Regarding compliance with data protection, it will take into account the compelling public interest in the current health emergency, including delays in responses (e.g. to data subject rights) due to diversion of resources to dealing with the virus [UK ICO]

Enforcement allowance

Controllers must:

- Evidence steps taken, challenges they faced and any other extenuating circumstances in relation to compliance
- Maintain suitable records of the actions that a controller has taken in complying with requests
- Communicate clearly with the individuals concerned about the handling of their request

[Isle of Man]



Fox Rothschild LLP
ATTORNEYS AT LAW

Deadline extension

- The deadline for submission of Certifications of compliance with cybersecurity requirements, and transaction monitoring and filtering programs, is extended by 45 days from the original due date.
- Several other deadlines were extended as well, but the extensions did not include the notification of a cybersecurity event within 72 hrs.

[NYDFS]

Delayed implementation

- Implementation of Brazil LGPD postponed until January 2021; enforcement to start only after August 2021.

[Brazil LGPD]

Delayed implementation?

- "Now is not the time to threaten business leaders with premature CCPA enforcement lawsuits," the organizations write. "A temporary deferral in enforcement of the CCPA would relieve many pressures placed on organizations due to COVID-19 and would better enable business leaders to make responsible decisions that prioritize the needs and health of their workforce over other matters."

[Letter to CA AG - CCPA]



Fox Rothschild LLP
ATTORNEYS AT LAW

Data Subject Rights

- Communicate with individuals: including any extension to the period for responding and the reasons for the delay. [DPC]
- Consider responding in stages. (e.g. electronic copies now; hard copy later)
- Communicate clearly. [DPC]
- Engage with individuals in order to ensure that the request is as specific as possible. [DPC]
- Ensure that the request is actioned as soon as possible. [DPC]
- Document the reasons for not complying with timelines [DPC]

Video Conferencing

- Use your contracted service providers (DPC)
- Ensure you are happy with the privacy and security features of the services (DPC)
- Ensure that employees use work accounts, email addresses, phone numbers, etc. (DPC)
- Provide clear, understandable, and up-to-date organizational policies and guidelines (what to use and how) (DPC)
- Implement, appropriate security controls (DPC)
- Prohibit and avoid sharing of company data, document locations or hyperlinks in any shared 'chat' facility that may be public (DPC)

TeleMedicine

- You MUST have a data processing agreement in place
- You MUST conduct a DPIA.
- CHOOSE a recognized video service with adequate protection

[Norway Datatilsynet]



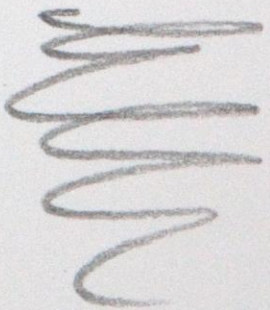
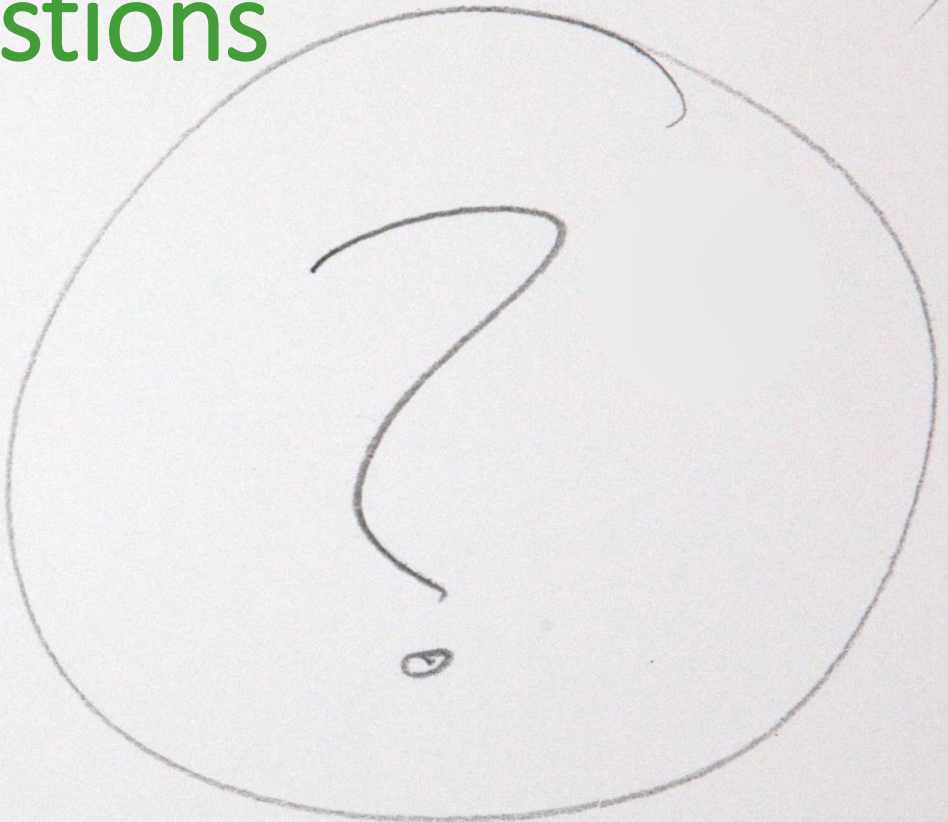
E-Learning

- ASK before using solutions not previously approved by the school.
- When use is done - delete all unnecessary information

[Norway Datatilsynet]



Takeaways and Questions



Odia Kagan

Partner, Chair of GDPR Compliance and International Privacy

Fox Rothschild LLP

okagan@foxrothschild.com

+1-215-444-7313

<https://www.linkedin.com/in/odiakagan/>

