



**The Effect of COVID-19 on GDPR -
What Directors Need to Know**
with Paul Lavery, Partner and Head of Technology and
Innovation, McCann FitzGerald
Morning and Evening Briefings Series: Kindly Sponsored by Mazars

 [@IoDIreland](#) [@MazarsIreland](#) [#IoDevents](#)

The Effect of COVID-19 and GDPR

- GDPR Recap
- COVID-19 and the GDPR –The Implications:
 - *GDPR Applicability in a time of crisis*
 - *Working from home – GDPR implications*
 - *Questionnaires and contact tracing for return to work (employees and customers)*
 - *Increased on-line services/sales*
- Potential future developments
- The Role of Data Protection Officer and interaction with board of Directors

GDPR Recap

- Replaced existing law in all member states on **25 May 2018**
- Designed to result in single, uniform set of data protection rules applying across the EU
- Retained and enhanced existing data protection concepts and requirements
- Increased obligations on controllers/processors
- Afforded new rights to data subjects
- GDPR represented an “evolution” of rights and obligations, but a “revolution” in respect of administrative compliance burden and sanctions for non-compliance
- Fines – Up to €20 million or 4% of worldwide turnover
- Second anniversary of GDPR imminent

GDPR Recap – Main obligations

- **Fair and Transparent Processing** – *data protection notices*
- **Legal basis for processing** - *consent, legitimate interests, performance of contract*
- **Purpose Limitation:** *Data to be kept for Specified, Explicit and Lawful Purposes and not further processed for any incompatible purposes*
- **Data Minimisation:** *Data should be adequate, relevant and not excessive*
- **Obligation to keep personal data accurate and up-to-date**
- **Record Retention and Deletion:** *Obligation not to retain data for longer than necessary*
- **Transfers outside EEA:** *prohibitions on transfers outside EEA – need to be able to rely on exemption such as consent, model clauses etc*
- **Access Rights** – *providing copies of personal data to data subjects on request*
- **Data Security** – *implementing and maintaining appropriate security measures against unauthorised access to, alteration, disclosure or destruction of personal data*

GDPR Recap – Main Obligations

- **Personal Data Breach Notifications** – *notification obligations to DPC and affected data subjects depending on whether incident is “risk” or “high risk” to data subjects*
- **Record of Processing Activities/Data Inventory** – *recording categories of data, categories of processing activities, categories of recipients, data transfers, retention times and security measures*
- **Documenting and Evidencing Compliance** – *Drafting and implementing relevant data protection policies and information notices; privacy by default and by design; data protection impact assessments*
- **Engaging Service Providers** – *Detailed data processing provisions required to be included in contracts*
- **Increased Data Subject Rights** – *access, rectification, erasure, data portability*

GDPR and COVID-19

- Time of crisis:
 - *Home/remote working*
 - *Video conferencing*
 - *Collecting data from employees or customers – for health and safety and/or contact tracing purposes?*
 - *Increased on-line services/sales*
 - *Key Consideration – The GDPR applies even in a time of crisis*

GDPR and COVID-19

- Processing during COVID-19 – Main GDPR Considerations:
 - *Data Security – avoiding personal data breaches*
 - *Fair and Transparent Processing*
 - *Legal Basis for Processing*
 - *Relevance and proportionality*
 - *Retention and deletion*
 - *On-Line sales and services – marketing obligations*

Remote Working

- Data Security – avoiding personal data breaches
 - *Directors should be conscious of data security risks and should also make staff aware of such risks*
 - *Confidentiality obligations still apply when working from home*
 - *Telephone calls and video conferences may be overheard by family, house mates and neighbours*
 - *Video calls may not be secure*
 - *Smart homes and virtual assistants (e.g. Alexa, Siri etc.) are constantly listening in – can be accidentally triggered and store record of conversations on their servers*
 - *Family and friends may see personal data and confidential information on computer screens*
 - *Print outs on printers may have highly personal or confidential information*

Remote Working

- Data Security – Tips
 - *Ensure appropriate policy in place in respect of home working (Dos and Don'ts)*
 - *Remind everyone of confidentiality obligations*
 - *Reminder not to use personal email accounts for work purposes*
 - *Ensure effective access controls in place – encryption, multi-factor authentication and ability to remotely wipe data stored on company devices in case of loss*
 - *Devices used for remote working should have the same levels of security as internal devices*
 - *Avoid ad-hoc use of video conferencing services unapproved by your company – verify the privacy and security features of the video-conferencing service chosen*
 - *Consider collection of confidential papers from director and employee households for confidential destruction*

Questionnaires and Contact Tracing

- Returning to work premises
 - *Ensuring a safe work place is likely to require checking with staff that they do not have COVID-19 symptoms and/or required to self-isolate*
 - *Questionnaire pre –work return*
 - *Ongoing questions after return?*
 - *Contact Tracing – e.g. recording what colleagues an employee mainly interacts with for contact tracing purposes*

Questionnaires and Contact Tracing

- GDPR Considerations
 - *Fair and transparent processing – ensure that data protection notices clearly refer to what data will be collected and the purposes of the processing*
 - *Legal basis for processing – may be preferable not to rely on consent:*
 - Legitimate interests (for personal data); and
 - for special categories of personal data (i.e. health data) - (i) processing necessary for carrying out employment rights or obligations (i.e. the requirement to ensure a safe work environment) or (ii) processing in the public interest in the area of public health or (iii) processing necessary to assess the working capacity of the employee.
 - *Relevance and proportionality – are all the questions relevant and proportionate for the purpose for which data is being collected?*
 - *Retention and deletion – ensure that data is not retained for longer than necessary*
 - *Consider whether data protection impact assessment is required*

Increased on-line services/sales

- GDPR Considerations
 - *Privacy Statement on website*
 - *Cookies policy*
 - *Marketing opt-ins and opt-outs*

What Now and what next?

- Increased number of DPC audits/investigations;
- Fines – DP Authorities will need to find their feet, ascertain appropriate fines – potential significant number of appeals?
- First DPC fine announced last week – Tusla (fined €75,000)
- Discovery of unintended consequences of GDPR and/or Data Protection Act that need to be rectified – potential that regulations will be drafted to facilitate processing of different categories of data
- Potential regulations to more clearly facilitate anti-bribery and anti-corruption due diligence
- Prospective new ePrivacy Regulation - marketing
- Increased data subject activism – complaints to DPC and cases against controllers

The Role of the Data Protection Officer

- Various entities are required to appoint a data protection officer (“DPO”) to oversee compliance with the Regulation:
 - *all public authorities (except courts)*
 - *bodies which are likely to be monitoring data subjects on a large scale*
 - *controllers or processors with large scale of special categories of data (e.g. health data)*
 - *other categories to the extent required by Member State law*

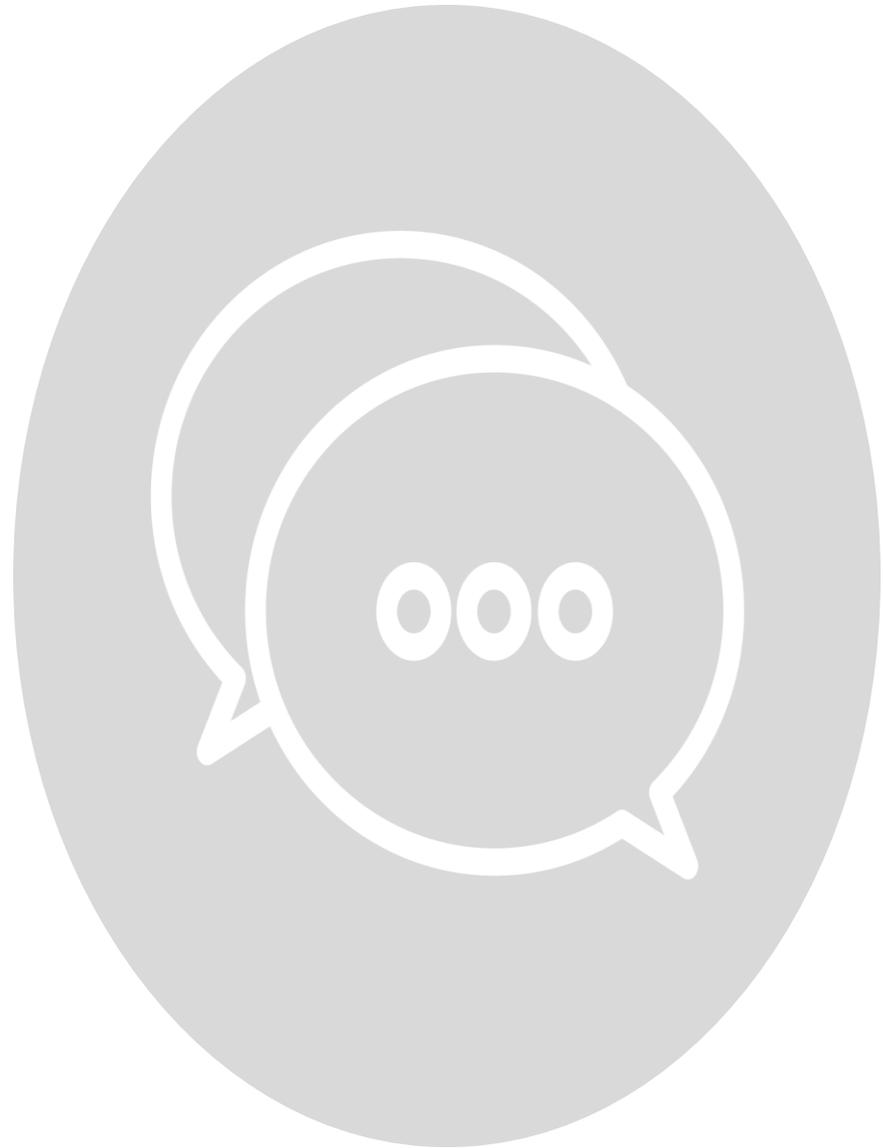
The Role of the Data Protection Officer

- Need to ensure that DPO is involved properly and in a timely manner in all issues relating to protection of personal data
- DPO must be provided with appropriate support and resources (internal and external support and legal advice)
- DPO must be independent (cannot receive instructions from employer/board regarding exercise of DPO functions)
- DPO cannot be dismissed or penalised for performing DPO tasks
- DPO shall report to highest management levels i.e. board of directors/CEO
- DPO may fulfil other tasks provided that the other tasks do not result in conflict of interest

The Role of the Data Protection Officer

- Inform and advise on data protection
- Monitor compliance with GDPR and policies and procedures
- Advice on data protection impact assessments
- Contact point for, and co-operation with, DPC

Questions?



Principal Office

Riverside One, Sir John Rogerson's Quay
Dublin 2 D02 X576
+353 1 829 0000

London

Tower 42, Level 38C, 25 Old Broad Street
London EC2N 1HQ
+44 20 7621 1000

New York

Tower 45, 120 West 45th Street, 19th Floor
New York, NY 10036
+1 646 952 6001

Brussels

40 Square de Meeûs, 1000 Brussels
+32 2 740 0370



Paul Lavery, Partner

McCann FitzGerald Law Firm

Head of the firm's Technology and Innovation Group

Email: paul.lavery@mccannfitzgerald.com

<https://www.mccannfitzgerald.com/people/paul-lavery>

Principal Office

Riverside One, Sir John Rogerson's Quay
Dublin 2 D02 X576
+353 1 829 0000

London

Tower 42, Level 38C, 25 Old Broad Street
London EC2N 1HQ
+44 20 7621 1000

New York

Tower 45, 120 West 45th Street, 19th Floor
New York, NY 10036
+1 646 952 6001

Brussels

40 Square de Meeûs, 1000 Brussels
+32 2 740 0370



**The Effect of COVID-19 on GDPR -
What Directors Need to Know**
with Paul Lavery, Partner and Head of Technology and
Innovation, McCann FitzGerald
Morning and Evening Briefings Series: Kindly Sponsored by Mazars

 [@IoDIreland](https://twitter.com/IoDIreland) [@MazarsIreland](https://twitter.com/MazarsIreland) [#IoDevents](https://twitter.com/IoDevents)