GDPR implications for the EU Institutions

7th May 2019

Paolo Sinibaldi, DPO European Investment Fund

EIF overview

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

The European Investment Fund (EIF) is an EU body, part of the European Investment Bank Group.

The EIF is established in Luxembourg and is specialist provider of risk finance to benefit small and medium-sized enterprises across Europe.

The EIF's shareholders are the European Investment Bank, the European Union, represented by the European Commission, and a wide range of public and private banks and financial institutions.

GDPR and EUDPR

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

EU Member States

Directive 95/46

GDPR - Regulation 2016/679

Applied since 25/5/2018

EU Institutions

Regulation 45/2001

EUDPR - Regulation 2018/1725

Applied since 11/12/2018

GDPR and EUDPR

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

GDPR recital n. 17 (emphasis added):

(…) *Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation.*

(…) ***the necessary adaptations*** *of Regulation (EC) No 45/2001* ***should follow*** *after the adoption of this Regulation,* ***in order to allow application at the same time as this Regulation****.*

GDPR and EUDPR

- EUDPR recital n. 4: *Regulation (EU) 2016/679 provides for the adaptation of Regulation (EC) No 45/2001 in order to ensure a strong and coherent data protection framework in the Union and to allow its application in parallel with Regulation (EU) 2016/679*.

- EUDPR recital n. 5 (emphasis added): *Whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU) 2016/679,* ***those two sets of provisions should****, under the case law of the Court of Justice of the European Union (the 'Court of Justice'),* ***be interpreted homogeneously****, in particular* ***because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.***

GDPR and EU Institutions

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

Some key changes introduced by GDPR were not new to EU Institutions (EUIs) as were implemented since 2001:

- Appointing a DPO (Reg. 45/2001 Art.24) - (GDPR Art.37)
- Keeping a register of the processing operations (Reg. 45/2001 Art.24.1(d)) – (GDPR Art.30)
- Making a risk assessment of the processing operations (Reg. 45/2001 Art.27.1) - (GDPR Art.35)

GDPR and EUDPR

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

GDPR	EUDPR
Independent Supervisory Authorities	
Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (Art 51.1)	With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies (Art.52.2) EDPS is in charge, inter alia, of: • Handling complaints from data subjects (EUDPR Art.63) • Carrying out data protection audits (EUDPR Art.58.1(b)) • Imposing administrative fines (EUDPR Art.66)

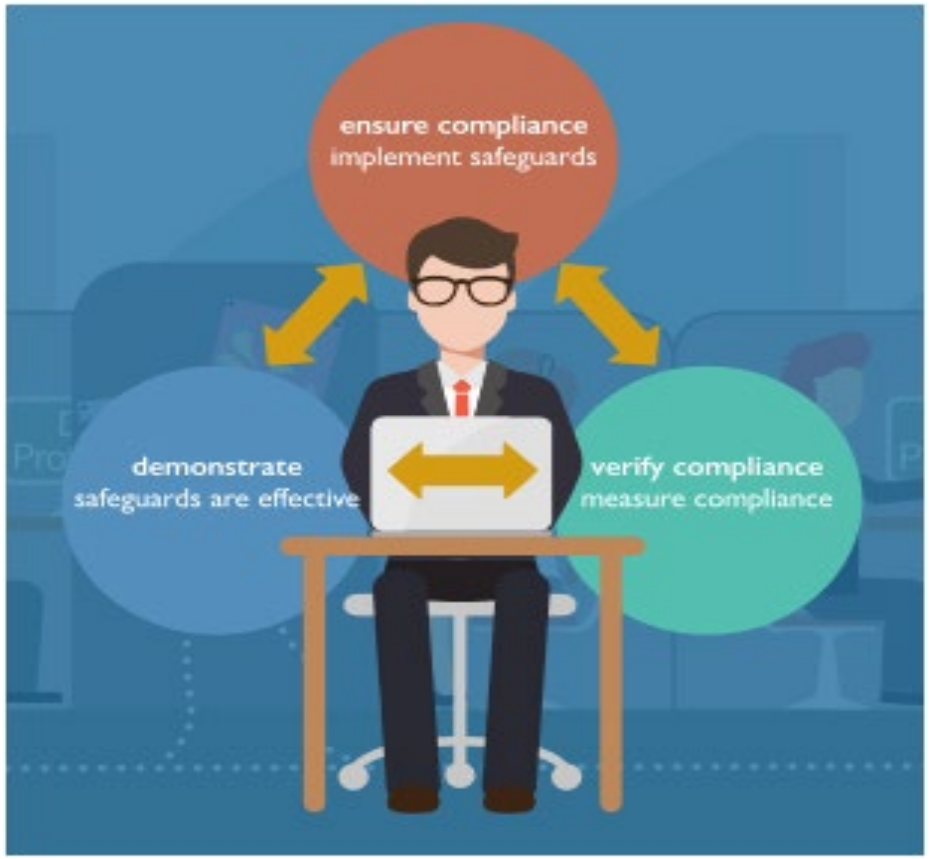
GDPR and EUDPR

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

GDPR	EUDPR
Administrative fines	
Art. 83 • Administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher • Administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher	Art. 66 • Administrative fines of up to 25 000 EUR per infringement and up to a total of 250 000 EUR per year • Administrative fines of up to 50 000 EUR per infringement and up to a total of 500 000 EUR per year

EU Institutions' DPO

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on



"Each EU institution, body and agency has a Data Protection Officer (DPO). Your DPO is your internal ally and can act as an adviser on data protection issues. If you want to avoid potential pitfalls, try to involve your DPO early on whenever you plan to work with personal data." (EDPS – "*New data protection rules for EU institutions and how they affect YOU*")

EU DPO's role: what has changed?

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

Reg. 45/2001

DPOs in charge of advising the controller, receiving prior notices and keeping a register of the processing operations.

Rule based approach - DPOs "notifying the EDPS of the processing operations likely to present specific risks…" (prior check notification to EDPS)

Reg. 2018/1725 (EUDPR)

DPOs DPIA advisors (Art. 39.2), no more in charge of the register (Art. 31) and with autonomous investigation rights (Art. 45.2)

Principle of accountability- risk based approach (EDPS prior consultation only in case of residual high risks) - Privacy by design/by default- Broader list of DPO's tasks

Examples of EUIs applying GDPR

LUXEMBOURG DATA PROTECTION DAYS 2019 GDPR, one year on

- EU Institutions acting as advisors of incorporated structures subject to GDPR
- EU Institutions appointed data processors on behalf of legal entities/controllers subject to GDPR
- Processing operations carried out by counterparties subject to GDPR on EU Institutions' representatives