GDPR in the Alternative Investment Sector

Everything you need to know to ensure compliance

CUMMINGS lawyers for alternative investments RFA Portman COMPLIANCE CONSULTING LLP

GDPR Essentials

- Who does the regulation apply to?
- What are the exemptions and derogations?
- What constitutes personal data?
- What is the difference between the data controller and the data processor

Evaluating your Existing Data

- Where is the data kept?
- Why do you have the data?
- Who does the data belong to?
- Do you have the subject's consent to hold the data?

Data Privacy Impact Assessment

- What is a DPIA?
- When should a DPIA be carried out?

Storing and Protecting Data

- Securing personal data
- Data protection by design
- Reporting data breaches

Deleting Data

- The right to be forgotten
- Subject deletion requests
- Data lifecycles

Updating Policies and Privacy Notices

- Internal
- External
- Client documents
- Stakeholder engagement

Compliance Landscape

- How does GDPR sit with other regulations?
- Data transfers between countries
- EU-US Privacy Shield
- MiFID II

The Cost of non-Compliance

- Article 83
  - Fines of up to 20m EUROS or 4% of total worldwide annual turnover of the preceding FY
- ICO can currently fine up to £500k
  - TalkTalk fined £400k after major data breach
  - Lead generation firm fined £260,000 for making 16.7m automated marketing calls
  - Nottinghamshire County Council fined £70k for not protecting personal information

Key Takeaways

- Carry out analysis of applicability
- Amend documents
- Policies and procedures
- Make appointments
- Technology review

Nancy King

Partner at Portman Compliance Consulting
Nancy@portmancompliance.com

Tel: 020 7205 2249

www.portmancompliance.com

Claire Cummings

Owner at Cummings Law
Claire.cummings@cummingslaw.com

Tel: 020 7585 1406

www.cummingslaw.com

George Ralph

Managing Director at RFA
gralph@rfa.com

Tel: 020 7093 5000

www.rfa.com

Questions

Q Would giving a business card or accepting an invite on Linkedin for instance can be considered as consent to hold contact details in a crm?

A Data held in the public domain, such as on LinkedIn or other social media is not covered under GDPR as it treats this as information where consent has already been given.

Business cards are different and the subject should be contacted separately to gain explicit consent for use. One way of doing this is by using a CRM add on which can mail everyone in the CRM system and ask for explicit consent to hold and use the information. Contact RFA for more information about this type of system, as there are many viable solutions out there and there may be one which suits your CRM and firm's requirements better than others.

Questions

Q You previously mentioned that taking data from public sources (eg a LinkedIn profile) would be permitted since it could be taken that the person tacitly consented to the use of that data by making it public. How does this dovetail with the changes to the definition of “consent” under GDPR?

A Data held in the public domain, such as on LinkedIn or other social media is not covered under GDPR as it treats this as information where consent has already been given. So the new consent regulations do not apply to that data if you can prove that it is available in the public domain.

Questions

Q What software is available to help us manage the data's lifecycle?

A There are many different options available to help you manage the lifecycle of your data. There are also some which can bolt onto your CRM system and allow you to request explicit consent from your data subjects which will then allow you to lawfully keep and use their personal data.

Some of those mentioned include: Consentric and Varonis but contact RFA for more information and a discussion about the best solution for your firm.