Impact of EU General Data Protection Regulation (GDPR) on marketing in financial services in the UK

May 2015

This hand-out has been produced with the kind assistance of Fieldfisher LLP . The law stated is correct as of this date. This does not constitute legal advice and it is highly recommended to seek professional legal advice when in any doubt about understanding your rights and obligations in order to comply with the law and regulations that impact marketing. Further information is available at www.godpo.eu

The journey to EU General Data Protection Regulation (GDPR)

The journey of the GDPR to the present day has been a long and at times controversial one. In January 2012, the European Commission (EC) issued a proposal for a European-wide data protection reform.

In March 2014, an amended proposal was approved by the European Parliament – in effect creating two drafts of the same Regulation (the Commission draft and the Parliament draft) with significant differences between them. Now we have a review of the proposals by the Council of Ministers who have declared that nothing is agreed until everything is agreed.

To date these drafts have had more amendments than any previous body of EU regulation and given the priority to gain consent on this landmark regulation by EC President Jean-Claude Juncker, many believe that the GDPR will be agreed by all parties by the end of 2015.

Although differences remain, most commentators believe that many business sectors and in particular the financial services sector can't adopt a 'wait and see' approach in the vain hope it will go away. It won't.

Data protection and the security of data is perhaps the biggest issue facing the sector from a business continuity perspective as to get this badly wrong opens the door to punitive fines of up to five percent of global turnover or €100m.

To underlie the vulnerability that large organisations have to becoming a victim of a data breach on grand scale, earlier this year both Facebook and Instagram were hacked by Lizard Squad, resulting in a 'denial of service attack' – denied by Facebook.

Either way, 1.6bn users of the social network couldn't access their accounts for over half an hour. Lizard Squad and other hackers like them represent a continuing threat to the data that financial services firms hold on servers that can be infiltrated by those who are determined to carry out such attacks.

Lizard Squad was also behind attacks on Sony and other major organisations

Under the new GDPR, data protection authorities (DPAs) will 'hold hands' and in doing so provide a so-called one-stop shop for complainants of financial services firms irrespective where the issue took place within the EU.

Change in existing EU data protection laws

Current Data Protection Directive 95/46/EC	Changes created by GDPR
European reach only	Global reach
Local law divergence across 28 EU states	Regulation: uniform across EU
Multiple Data Protection Authority ("**DPA**") exposure	"One stop shop"
Limited accountability	Accountability key!
Controllers only	Controllers and Processors
Small fines, differ between countries	Huge fines
No obligation to report breaches	Obliged to report breaches without delay
No obligation to have DPO	DPO required for larger organisations

The GDPR will effectively replace the former Data Protection Directive 95/46/EC as well as make the existing Data Protection Act 1998 redundant by bringing in a European-wide approach to data protection and security that moves away from the patchwork approach that exists at present. It also places data processors and data controllers with equal legal responsibilities with respect to the transfer and use of data.

A proposed 'data protection seal' will notify consumers that the financial services firm complies with the supervisory authority and can transfer data to third parties on a lawful basis in the hope that consumers will be reassured about the higher standards of data protection that such a firm complies with.

The obligation to report breaches – however small – will be the responsibility of the Data Protection Officer (DPO) who will work independently within a large financial services organisation and the reporting of such breaches is likely to be done within 24 hours.

EU Ordinary Legislative Procedures

- Initial consultation
- Institutional feedback
- Agrees text

- Committee appointed (LIBE)
- Various reports commissioned
- Amendments to Commission version
- 1st reading: agrees text in full Parliament vote

- Working party appointed (DAPIX)
- Series of meetings reviewing text
- 1st reading: agrees Parliament text or proposes amendments

- "Trilogue" formed from all three institutions
- Text goes back to Parliament for a 2nd reading and, if necessary, back to Council for a 2nd reading
- If Council rejects the Parliament's amendments, a Conciliation Committee is set up. If can't agree joint text here, dropped
- Text agreed this is sent to Parliament for a 3rd reading and then to Council

Adopted

Rejected

Timetable for GDPR

Many commentators have remarked on the problem of the slippage in the timetable to introduce the GDPR. The lack of clarity makes it hard for firms to plan and prioritise what is important and it's easier to do this once things are nailed down.

In addition, there's also a concern that good data controllers are being punished as they are more likely to report breaches. On the other hand, the forthcoming GDPR will give more clarity to marketing activities within the financial services sector and this has to be in the best interest of its customers.

Summary of main changes made by GDPR within EU law

Main change	Description
Territorial scope	Extended to organisations outside of EU processing data related to EU citizens (includes offering services or monitoring)
One stop shop	Replaces 'lead authority'
Supply chain	Controllers and Processors and 'Data Protection Seal'
Increased fines	Up to 5% global turnover/€100m
Data breach reporting	Without undue delay
Data Protection Officers	Appointed where data processed >5,000 records
Privacy Impact Assessments	At least annually (and consultation with DPA/supervisory authority)
Consent	Must be freely given and obtained for a specific purpose
Security broadened	More than 'technical and organisational measures'
Personal data	Includes cookies and IP addresses
More transparency	Icon-based privacy notices
Pseudonymous and encrypted data	Still personal data but subject to less stringent requirements
International transfers	Adequacy criteria is amended by GDPR

Issue of Customer Consent

The issue of customer consent is currently a hot topic within financial services and it's clear that banks such as HSBC are re-wiring their approach from the position of protecting the customer as the paramount principle in how they manage their business.

Financial services firms must obtain consent and this must be freely given for a specific purpose rather than for some blanket purpose.

There is still some argument between lawyers as to whether implied consent is a 'dead duck' – and some lawyers feel that implied consent in certain circumstances will still be lawful under the GDPR.

Major causes of a data breach

Human error accounts for the biggest cause of data breaches in financial services

A major cause for a data breach can be identified as human error and clearly the issue of education and training will be core to the way in which this risk within financial services can be reduced.

However, there is increasingly recognition, particularly with junior staff, that such a risk could never be 100% eradicated, leaving open the possibility of fines and sanctions as a real possibility under the GDPR.

Typical human error includes the failure to encrypt data, a lack of privacy policies and even mis-directed communications, whether post, fax or email.

In one case, the sender had accidentally clicked 'Reply all' that had sent a private email beneath the message to be read by over 55m other people before the matter was brought under control.

And of course by then it was too late and a significant data breach had occurred.

Most common grounds for taking enforcement action for data breach

- Human error
- Failure to encrypt
- Lack of policies
- Lack of staff training
- Misdirected communications (fax, email, post, hand delivery)
- Reliance on electronic systems
- Paper records
- Accidental loss / theft
- Breaching direct marketing rules
- Bad asset control (decommissioning of hardware)

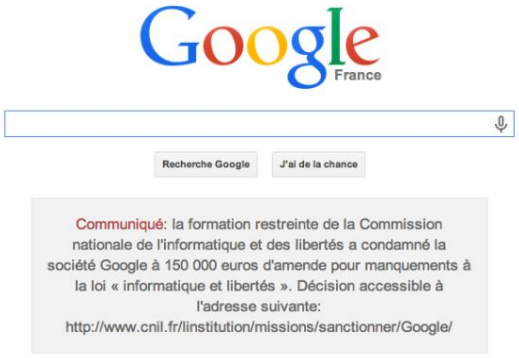
Most common grounds for mitigation for data breach

- Self-reported to Data Protection Authority (DPA)
- Good post-incident behaviours:
  - Detailed investigations after breach
  - Remedial action
  - Cooperated fully with DPA
- Most organisations that were fined are good data controllers!

Negative media coverage can damage brand value

As well as fines, DPAs like to 'name and shame' those firms that have fallen below the standards expected of them and the reputation damage to the brand in such cases could easily outstrip the financial penalties imposed.

For example, the French authorities recently forced Google to publish details on non-compliance on its home page for 48 hours. Google complained but lost its case in the courts.



BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

The Financial Conduct Authority's Conduct of Business Source book (COBS) that governs marketing within the financial services sector will need to be revised in light of the GDPR.

For example, terms and conditions in contracts will need to be fair, clear and not misleading and an audit done by her firm on the websites of many of the delegates attending the seminar showed massive failings in this area.

The language in privacy policies can no longer read like gobbledygook and must be clear for those who are intended to read it, particularly with regard to asking for their consent. And the gap between how the rules apply to B2C and B2B will narrow as to become invisible altogether.

Top 10 Tips for marketing professionals in financial services

1. Write down a set of data protection policies and procedures and ensure that these are compliant with the GDPR. Such policies and procedures should include what actions need to happen in the event of a data breach.

2. Consider what breaches might do harm to customers/clients and pay particular attention to mitigating these risks. The most serious are either financial fraud or identity fraud, so sales and marketing professionals should pay particular attention to passport details and other personal information stored on their servers.

3. All financial services firms need to invest in education and training all employees involved in collection and processing of data with a view to reducing the risk of human error and as far as possible try and automate as many processes as possible in order to reduce the risk of human error.

4. All financial services firms need to set very clear, fair and transparent rules for obtaining customer consent.

5. All financial services firms shouldn't keep data forever – unless of course it's to ensure that they don't contact someone who has expressly said that they don't want to be contacted in the future and not having such information could lead to them being contacted again by accident.

6. All financial services firms should have a policy for destroying out-of-date data.

7. All financial services firms need to recognise the risk of consumer activism where one aggrieved customer can very quickly galvanise a mass campaign against the brand on Twitter and social network sites.

8. Sales and marketing professionals need to integrate data protection fully into all business processes and not treat this as an add-on or side issue.

9. Marketers should consider the GDPR as a marketing opportunity and potentially a source of competitive advantage by performing data processing tasks more efficiently and accurately.

10. Customers should be treated as a source of business rather than a piece of data and need to be treated fairly, with respect to their rights to privacy and without cynicism.

About the authors

Ardi Kolah FCIM LL.M is co-author of Data Protection and Privacy: A practical guide to complying with the EU General Data Protection Regulation and The Data Protection Officer's Handbook: Your guide to the skills and knowledge required under the EU General Data Protection Regulation to be published by Kogan Page in early 2016. He's also Commissioning Editor of the Data Protection and Privacy Toolkit, to be published in 2015 by Kogan Page.

He's Chairman of the Law & Marketing Committee, Worshipful Company of Marketors in the City of London and co-founder of GO DPO® a specialist executive training and recruitment company owned by EU Compliance and Recruitment that provides support for the new breed of Data Protection Officers provided under the EU General Data Protection Regulation. Ardi is a Member of the IAPP.

Martin Hickley is a consultant to GO DPO® and data governance, protection and privacy specialist with 25 years' of experience mediating with regulators (FCA, ICO, DVLA and Dep Ed) in the world of data and information, working in blue chip companies where data is the raison d'être of the organisation.

Experienced in data management, data governance, privacy, risk, compliance and security he takes a global and enterprise view of how data should be fashioned to meet all known current and future business objectives within the evolving regulatory framework. Martin is a Fellow of the British Computer Society.