NICE · ACTIMIZE

Financial Crime and Compliance under GDPR

Richard Malish, General Counsel and Head of Partnerships, NICE Actimize

White Paper

Europe's revised privacy regime, the EU General Data Protection Regulation (GDPR), will become effective on 25 May, 2018. While GDPR is a major enhancement to Europe's existing privacy framework, soundbites and summaries painted with too broad a brush have caused many to believe that all personal data processing is now endangered. For those of us in the financial crime and compliance arena, it is often difficult to get a realistic view of the impact of GDPR on processing personal data to protect our customers, companies and financial systems.

Financial services firms and compliance professionals have had to ask whether GDPR requires consent to process data to protect against fraud, money laundering and trading compliance risks. If customers have the right to have their data erased, does that put us at risk of erasing data necessary to help predict future suspicious activity? And how does GDPR relate to all of the conflicting regulatory regimes that force us to keep and process data?

This whitepaper addresses the impact of GDPR on certain aspects of financial crime and compliance prevention. The aim is to help your organization manage the discussion with various stakeholders and customers, along with your own legal counsel, about how GDPR impacts your use of NICE Actimize solutions as well as similar points and alternative financial crime solutions.

Our analysis is based on our own data protection impact assessment, advice from expert personal data and privacy counsel and consultants, discussions with our clients and review of GDPR provisions in contract addendums and RFPs from financial services firms. NICE Actimize's unique position as the leader in financial crime solutions among a diverse financial institution client base gives us the ability to aggregate the market's response and concerns, and we are proud to share those insights here.

What is GDPR?

The General Data Protection Regulation is Europe's replacement of the 1995 Data Protection Directive and its new primary regulation governing data privacy. Its goal was to harmonize the national data privacy laws that had been implemented pursuant to the Directive, as well as expand certain protections in line with evolving European standards.

While there has been strong privacy protections in Europe for over two decades, the changes imposed by GDPR and the increased potential liability imposed thereunder have caused many covered entities to plan and invest in data protection like never before.

What has changed from existing data protection regulations?

There are many commentators who focus on the similarity between GDPR and existing European data protection law, and dismiss the hyperbolic claims of privacy consultants eager to sell their services. There's no doubt there is some truth in their scepticism.

However, the reality is that some companies treated the existing regulations as lower priority when considering commercial interests or the multitude of other new regulations imposed over the last 20 years.

The GDPR makes failure to comply with some aspects of the regulation subject to administrative fines equal to the higher of €20 million and 4 percent of the total worldwide annual turnover of the preceding financial year. These potential fines have changed the risk-reward analysis and the scales have now been tipped to make data protection a dominant factor in any processing decision.

In addition to the fines, there are several additional obligations which may have significant impacts. For example, most financial services firms will be required to designate a data protection officer with expert knowledge of privacy law.

Consent for most personal data processing may no longer be assumed, but must be "by a statement or by a clear affirmative action,"[i] specific to the operation requiring such consent and can be withdrawn at any time. GDPR also imposes stricter obligations on data security and specific breach notification guidelines. Add to this mandates for technological solutions and processes to be designed with privacy in mind, and the need to pass certain obligations on to their processors, then you will understand why financial services firms cannot be complacent.

How have banks prepared for GDPR?

GDPR was adopted in 2016 and a two-year lead time was provided to give companies the time necessary to adapt their business methods, policies and vendor relationships. However, many financial services firms have not had the time to focus on GDPR as they were focusing on implementing the Market Abuse Regulation (**MAR**), effective 3 July 2016, and the Markets in Financial Instruments Directive (**MiFID**) II, effective 3 January 2018, as well as the fallout from Brexit. Many U.S. financial institutions, still managing compliance changes imposed by Dodd-Frank, were happy to neglect GDPR until the market started focusing on it over the last few months.

From NICE Actimize's experience, while financial services firms may have undergone change management on certain non-financial crime-related functions earlier, requests to modify vendor relationships started in earnest in March of this year. We expect to continue to engage our clients on reviewing our master agreements and other aspects of how Actimize solutions can help clients become GDPR compliant. Luckily, we have already done a lot of the heavy-lifting to address future concerns as detailed herein, and we have and will continue to design data protection into our solutions.

How does GDPR impact fighting financial crime?

Financial services firms will often act as "controllers" of the personal data they collect on customers and counterparties. Controllers are obliged to respect and facilitate the multitude of privacy rights granted to individuals, or "data subjects," granted under GDPR. However, while financial services firms may need to reengineer and restrict their processing of personal data for activities such as marketing, they are provided much more leeway when fighting financial crime.

Lawfulness of processing

Article 6 - Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
…
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data….

Much that has been written about GDPR relates to the burden of obtaining proper consents to process data. This general theme has bled into discussions about financial crime to the point of creating questions about whether and how financial services firms can process data to fight financial crime if they need consent of the data subject.

While there are certainly valid questions, GDPR is much more permissive to the extent data is used to prevent or monitor for financial crime.

In many cases, clients and counterparties are willing to consent to the processing of their data to receive or participate in financial services. But consent can be withdrawn, so asking individuals to consent will give the impression that they can exercise data privacy rights, such as the right to erasure, which may not be appropriate for highly-regulated activities.

Rather than relying on consent, the GDPR also permits (1) processing which is necessary for compliance with a legal obligation to which the controller is subject and (2) processing which is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

Some areas of financial crime prevention are clearly for the purpose of complying with a legal obligation. For example, in most countries there are clear local law obligations requiring the monitoring of financial transactions for suspicious activity to fight money laundering and terrorist financing.

The European Data Protection Supervisor stated in 2013 that anti-money laundering laws should specify that "the relevant legitimate ground for the processing of personal data should… be the necessity to comply with a legal obligation by the obliged entities, competent authorities and FIUs."[ii] The 4th EU Anti-Money Laundering Directive requires that obliged entities provide notice to customers concerning this legal obligation, but does not require that consent be received. The UK Information Commissioner's Office gave the following example of a legal obligation which constitutes a lawful basis:

> *A financial institution relies on the legal obligation imposed by the Part 7 of Proceeds of Crime Act 2002 to process personal data in order to submit a Suspicious Activity Report to the National Crime Agency when it knows or suspects that a person is engaged in, or attempting, money laundering.*[iii]

The UK ICO also clarified that the requirement that processing be "necessary" for compliance with a legal obligation does not mean "essential." Rather, "it must be a reasonable and proportionate way of achieving compliance."

Very few commentators have attempted to cite a legal authority for anti-fraud legal obligations. The Payment Services Directive 2 (PSD2) requires that EU member states permit processing of personal data

by payment systems and that payment service providers prevent, investigate and detect payment fraud.[iv] But PSD2 has its own requirement for consent and this protection may fail without adequate implementing legislation in the relevant jurisdiction. Another possible angle is that fraud is a predicate offense for money laundering, and therefore the bank has an obligation to investigate fraud to avoid facilitating money laundering.

Rather, fighting fraud is generally seen as a "legitimate interest." As discussed below, "legal obligations" are preferable to "legitimate interests" as a basis for personal data processing. While the financial services industry is unlikely to desire many more legal obligations, having a more definitive obligation to perform anti-fraud activities may be helpful to justify anti-fraud data processing activities under GDPR.

"Legitimate interests" are also permitted as a basis for processing. However, this basis can be challenged where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Financial services firms may not feel comfortable threading the needle between these ambiguous competing interests.

Fortunately the GDPR makes clear that several purposes related to financial crime should be considered legitimate interests, which can at least bolster any arguments against the legality of the processing. For example, "the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned"[v] and profiling for the purposes of fraud prevention may also be allowed under certain circumstances.[vi]

While this is relevant to traditional fraud protection processes, it is also worth recognizing that many financial market crimes such as insider trading, spoofing and layering are oftentimes prosecuted under anti-fraud statutes.

Compliance with foreign legal obligations, such as a whistle-blowing scheme required by the US Sarbanes-Oxley Act, are not considered "legal obligations" for processing under Article 6(1)(c), but they should qualify as legitimate interests.[vii] Processing data beyond an originally-intended purpose and transmitting the data to competent authorities is also considered legitimate if the data indicates "possible criminal acts or threats to public security."[viii]

While legal obligations and legitimate interests do not cover all potential use cases, they should cover most traditional financial crime and compliance processing. Some financial services firms have been informing their clients that a legal obligation justifies their processing for anti-money laundering, anti-fraud and the assessment and management of more general bank risks. Others have included legal obligations, legitimate interests and even the necessity to perform a contract as all potential justifications for a laundry list of potential processing activities.

Financial services firms should use the remaining days before GDPR's effective date to provide the correct notifications to data subjects and confirm that their processing adequately falls under a defensible basis for processing. And with this basic housekeeping performed there is hopefully little disruption to their ability to process data for financial crime and compliance operations.

Right of access by the data subject

The right of individuals to file a "Subject Access Request" to receive access to the personal data held by controllers is an existing right under pre-GDPR EU privacy law. However, GDPR removes the right to charge a fee for responding in most circumstances, limits the time limit for a response to 30 days and expands the content to be provided.

The expansion of this right, which already is a substantial responsibility similar to the painstaking discovery and redaction process in litigation, will likely continue to consume financial services firms' already strained resources.

However, the obligation to provide processed personal data may be limited if it "adversely affects the rights and freedoms of others." The GDPR recitals make clear that this goes beyond personal data rights, but also rights such as "trade secrets or intellectual property and in particular the copyright protecting the software."[ix] It may be possible to understand the underlying IP in a software solution by analysing the derived data disclosed pursuant to one or several Subject Access Request. It is also risky because it may reveal the gaps in a firm's surveillance capabilities which can be exploited.

It would be helpful if the EU or the member states can clarify, as some have in their national legislation,[x] that protecting data subjects against financial crime threats is an equal or greater right that trumps the right to receive access. For anti-money laundering, the 4th EU Anti-Money Laundering Directive makes clear that "access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing" and requires that Member States "adopt legislative measures restricting, in whole or in part, the data subject's right of access to personal data." Instead, the data subject has the right to request that a supervisory authority confirm the lawfulness of the processing.

Article 15 - *Right of access by the data subject*

(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- *a) the purposes of the processing;*
- *b) the categories of personal data concerned;*
- *c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
- *d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*

…

- *g) where the personal data are not collected from the data subject, any available information as to their source;*
- *h) the existence of automated decision-making, including profiling, …, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*
- *i) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards*

….

(3) The controller shall provide a copy of the personal data undergoing processing.

(4) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Right to erasure

The right to erasure, or the right to be forgotten, attracted the attention of the world because of a 2014 ruling in which a Spanish citizen won the right to have data on him deleted from Google. That case was tried under data privacy constructs that pre-dated GDPR. GDPR has now enshrined that right into its own article in the data privacy law.

Individuals have the right to have their personal data erased upon request if, among other potential justifications:

- The data is no longer necessary for the original purpose;
- Consent is necessary for processing, and the individual withdraws their consent; or

- Processing is based on legitimate interests, but the individual objects and there is no overriding legitimate interest to continue processing.

These exemptions from the right of erasure highlight the importance of trying to find justifications for processing which do not rely on consent or ambiguous legitimate interest arguments.

Relying on a valid legal obligation is the most suitable and protective justification for fighting financial crime and compliance purposes. There are several potential legal obligations for financial services firms to rely on.

Article 17 - *Right to erasure*

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;….

(b) the data subject withdraws consent on which the processing is based …, and where there is no other legal ground for the processing;

(c) the data subject objects to the processing … and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing ….

- MiFID requires firms to keep records for at least five years (and in seven years in some circumstances) and no more than 10 years from the relevant transaction. Customer due diligence must be expunged after five years from the end of the customer relationship unless there are ongoing court proceedings or there are reasonable grounds to believe that the records need to be retained for legal proceedings.
- MAR requires personal data to be retained for a maximum period of five years.[xi]
- The 4th EU Anti-Money Laundering Directive requires retention of customer due diligence information and supporting evidence and records of transactions for five years from the end of the applicable relationship, and EU member states can allow for another five year period "where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing."[xii]

Foreign legal obligations are not recognized as "legal obligations" capable of shielding the controller or processor from complying with the erasure request. However, they may qualify as overriding legitimate interests.[xiii]

The UK Financial Conduct Authority has attempted to clarify that its data retention policies trump the GDPR. A spokesman for the Financial Ombudsman Service also tried to clarify that requests to delete data should be considered in relation to the firm's "usual data retention policies and if the data is something that can be deleted."[xiv] However, they also left open the possibility that extraneous information such as "unnecessary medical information" might need to be selectively expunged. Financial services firms should attempt to limit collection and processing of such data on the front end in order to avoid the need to clean out select information within individual accounts.

Article 5 - *Storage limitation*

(1) Personal data shall be:…

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed….

Storage limitation

The storage limitation obligation of GDPR is very similar to the right of erasure. This right protects all of us who either have more pressing matters than to exercise our right to be forgotten or are too lax with their personal

information to recognize the harm until it is too late.

The storage limitation now requires controllers to make sure that they determine the retention period necessary to retain the personal data. Retention periods required by law as detailed in the Right of Erasure section will generally control.

While this seems reasonable when managing a file cabinet, this presents very difficult issues when you consider that many financial institutions have multiple data repositories, systems of record and now data lakes for big data analytics. Financial services firms which have not considered how their systems can automate such purges may find it difficult to rely on manual processes.

Financial services firms should recognize that in many cases the retention period caps are based on details which are not known by the financial crime solution. For example, although the financial institution may determine to set their customer due diligence retention period default to five years from the end of the relationship in line with the 4th EU Anti-Money Laundering Directive, they will not be able to guess that date when it engages its customer due diligence solution throughout the relationship. This status will only exist in upstream systems that feed to downstream financial crime systems. Therefore, financial services firms should consider whether changes in customer status from upstream systems can be feed into downstream systems for deletion at a later time.

It is also possible that custom data stores created outside of or in addition to out-of-the-box software may not respond to automated deletion functionality as expected. Financial services firms should engage their software vendor or system integrators to perform a health check of the entire architecture surrounding each point solution.

Right of rectification

GDPR includes a right for data subjects to have inaccurate personal data corrected. It is perhaps the GDPR principle with the least amount of commentary – to many people it probably appears like a binary issue of correct or incorrect. And most systems and solutions will probably be able to permit rectification on a go-forward basis.

Article 16 - *Right of rectification*

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

But the right of rectification arguably poses a significant problem for financial institutions in regard to historic processing. Many financial institutions are under an obligation to keep all files in their original form under Dodd-Frank's WORM (write once read many) rules or general audit trail obligations. If an alert for suspicious activity is generated based on incorrect data, no compliance professional or regulator would likely advise that the alert, its disposition or a subsequent filing to a regulator could be erased. It would also be beyond the technological state of the art, and beyond most people's expectations, to attempt to rectify every personal detail that might be recorded as part of a trader's communications surveillance. Records based on incorrect data will likely continue to be processed as part of historic trend or look-back reviews.

The UK ICO has given some comfort that the mistake captured in prior data processing "is, in itself, accurate and should be kept" and the incorrect data should be kept along with the corrected information.[xv] The ICO gives the example of keeping the misdiagnosis of a patient in the file as the accurate record of

the patient's medical treatment: "As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified."

Similar misdiagnosis scenarios are likely to happen in the financial crime and compliance sector. For example, a suspicious activity alert based on false beneficial ownership or a fraud alert based on an account incorrectly tagged for potential fraud. In both cases it will be important for the financial services firm to be able to understand its prior activity, or lack of activity, based on such information believed at the time.

In the absence of further guidance or restrictions to this right under EU or Member State law, financial institutions will likely rely on the same legal obligation and legitimate interest arguments mentioned above to justify any ongoing storage or processing of incorrect data for periods prior to the correction date.

While outside the scope of this paper, it is worth noting that the rights of rectification and erasure also raise interesting questions when considering blockchain-enabled financial crime systems in which personal data stored on the blockchain are immutable. Financial services firms will need to carefully vet their control over any such system to the extent personal data cannot be rectified or deleted.

Right to Data Portability

Article 20 - *Right to Data Portability*

(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means….

Data portability is a new fundamental right with the purpose to "empower the data subject and give him/her more control over the personal data concerning him or her."[xvi] For those of us yet to suffer from vendor lock-in due to data, the concept can be analogized to the economic freedom granted to consumers when we were granted the right to port our cellphone numbers to competing carriers. Data portability is also intended to foster competition and new services, similar to the granting of access to banking records under Europe's PSD2.

However, this new right is only relevant if the data is processed based on the data subject's consent. As discussed, consent may not be necessary for processing data for financial crime prevention, and therefore there is no need to give data subjects the right to port this data to a third party.[xvii] The Article 29 Data Protection Working Party has been explicit in this regard:

> There is no obligation for financial institutions to answer a data portability request concerning personal data processed as part of their obligations obligation to prevent and detect money laundering and other financial crimes….[xviii]

It is also important to note that the applicable data is limited to that which the individual "provided" to the controller. The Article 29 Working Party has given examples of music playlists and purchases using certain loyalty cards. Data provided by individuals will generally not be primarily stored in the financial crime software solution but rather in an upstream database. Processed data, such as suspicious activity reports, are out of scope and therefore may be in a proprietary format.

Data protection by design and default

The principles of data protection by design and default tie together the full range of GDPR concerns and places them at the forefront of the financial services firms' relationship with their financial crime solution partners.

GDPR imposes new mandates on data controllers to implement technological and organizational measures designed to fulfill data protection principles ("privacy by design") and to ensure that only data necessary for each specific purpose is processed by default ("privacy by default"). These requirements elevate the discussion with software vendors from asking whether they comply with GDPR, to whether the software itself allows the controller to fulfil their data protection obligations.

Article 25 - *Data protection by design and default*

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Unfortunately there are few substantive guidelines for what these concepts mean and the Article 29 Data Protection Working Party has not yet provided additional context. It appears that the drafters were willing to take a flexible approach, since privacy by design is to be weighed against "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing." Anyone familiar with the complexity and cost of managing bank systems could be forgiven for imagining the reference to cost would outweigh all of the other factors. But given the important of privacy in the EU, it is probably prudent to assume that these caveats simply will result in forcing companies to use the prevailing state of the art as opposed to paying for the most cutting-edge technology.

The first step for financial services firms prior to engaging with suppliers will be to adopt policies and measures which strive to meet the obligations which are agnostic to technology solutions. This could include, among other measures, minimizing the processing of personal data, pseudonymizing personal data "as soon as possible" and being transparent with individuals in regard to the functions and processing of personal data.[xix] The good news is that existing laws and regulations, such as the current EU Data Protection Directive and bank secrecy laws, already require extensive privacy safeguards and many of these measures should already have been contemplated.

These standards can then be leveraged for functional requirements documents used when implementing new technological solutions. If financial services firms are able to manage these processes in their customer-relationship management or other systems of record, then there should be fewer instances where the process needs to be recreated or the data scrubbed from within the financial crime platform.

Staying GDPR Compliant with NICE Actimize

As the above discussion makes clear, financial services firms have an overabundance of conflicting interests and concerns that need to be balanced when implementing GDPR. While there will be questions of interpretation, the carve-outs and protections for processing personal data for financial crime and compliance should hopefully make implementation less onerous for compliance departments than perhaps other departments within financial services organizations. NICE Actimize has created technical documentation to assist in your analysis that is available upon request, and we are continuing to develop tools to help automate and simplify on-going data privacy processes. We encourage you to reach out to your account executive to determine how NICE Actimize can help your firm maintain compliance with GDPR.

Ready to learn more?

Get in touch: info@niceactimize.com

Staying GDPR Compliant with NICE Actimize

As the above discussion makes clear, financial services firms have an overabundance of conflicting interests and concerns that need to be balanced when implementing GDPR. While there will be questions of interpretation, the carve-outs and protections for processing personal data for financial crime and compliance should hopefully make implementation less onerous for compliance departments than perhaps other departments within financial services organizations. NICE Actimize has created technical documentation to assist in your analysis that is available upon request, and we are continuing to develop tools to help automate and simplify on-going data privacy processes. We encourage you to reach out to your account executive to determine how NICE Actimize can help your firm maintain compliance with GDPR.

ABOUT NICE ACTIMIZE

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

info@niceactimize.com | niceactimize.com/blog | @NICE_actimize | /company/actimize | NICEactimize

NICE · ACTIMIZE

Citations

[i] EU General Data Protection Regulation 2016/679 (**GDPR**), Article 4(11), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[ii] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* (4 July 2013), https://edps.europa.eu/sites/edp/files/publication/13-07-04_money_laundering_en.pdf.

[iii] UK Information Commissioner's Office, *Legal Obligation*, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/.

[iv] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (25 November 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.

[v] GDPR Recital 47.

[vi] GDPR Recital 71.

[vii] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (9 April 2014), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[viii] GDPR Recital 50.

[ix] GDPR Recital 63.

[x] Irish Data Protection Act, 1988, Section 5, http://www.irishstatutebook.ie/eli/1988/act/25/section/5/enacted/en/html#sec5.

[xi] Market Abuse Regulation (596/2014), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0596&from=EN.

[xii] Fourth Anti-Money Laundering Directive (EU) 2015/849, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES.

[xiii] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (9 Apr 2014), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[xiv] FT Advisor, *FCA rules trump EU data deletion law* (18 April 2018), https://www.ftadviser.com/your-industry/2018/04/18/fca-rules-trump-eu-data-deletion-law/.

[xv] UK Information Commissioner's Office, *Right to rectification*, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/.

[xvi] Article 29 Data Protection Working Party, *Guidelines on the right to data portability* (5 April 2017), https://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

[xvii] GDPR Recital 68.

[xviii] Article 29 Data Protection Working Party, *Guidelines on the right to data portability* (5 April 2017), https://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

[xix] GDPR Recital 78.

ABOUT NICE ACTIMIZE

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

info@niceactimize.com | niceactimize.com/blog | @NICE_actimize | /company/actimize | NICEactimize

NICE · ACTIMIZE