ARTICLE

EU GDPR COMPLIANCE WITH FIS CONSENT MANAGER

ARTICLE SUMMARIES & SOLUTIONS

ARTICLE

EU GDPR COMPLIANCE WITH FIS CONSENT MANAGER

ARTICLE SUMMARIES & SOLUTIONS

FIS Consent Management to GDPR Articles

The EU GDPR regulation, which will be enforced from 25 May 2018, revolutionises the data privacy landscape in Europe. GPDR gives individuals greater control and transparency over their personal data and raises the bar for businesses to achieve lawful processing of personal information. Compliance will require more than technical solutions, as it will be necessary for businesses to change their mindset and culture to one that recognises the primacy of an individual's rights over their data.
This whitepaper outlines how, using the FIS Consent Management platform, businesses can simply and quickly solve eleven key articles of the incoming regulation, avoid heavy fines and sanctions as well as empowering customers with enhanced, personalised services.

FIS Consent Management is an indispensable partner in the development of a GDPR solution because it enables a business to have a dynamic and transparent data relationship with individual customers. It empowers customers to control how their data is processed, allows business systems to have a real-time knowledge of data rights to determine if lawful processing is possible and equips the business' Data Protection Officer (DPO) with tools to monitor and deliver on a business's privacy promises and obligations.

- **A rticle 4.11:** Consent definitions
- **Article 6:** Lawfulness of processing
- **Article 7:** Conditions for consent
- **Article 8:** Conditions applicable to child's consent in relation to information society services
- **Article 9:** Processing of special categories
- **Article 15:** Right of access by the data subject
- **Article 16:** Right to rectification
- **Article 17:** Right to erasure 'right to be forgotten'
- **Article 20:** Data portability
- **Article 21:** Right to object
- **Article 24:** Responsibility of the controller to demonstrate compliance

Article 24: Responsibility of the controller to demonstrate compliance

GDPR places a higher burden on businesses to demonstrate compliance. "The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation" **(Article 24)**. Importantly, supervisory authorities are required to consider both the organizational and technological measures that have been implemented **(Article 83)** when determining the severity of non-compliance fines.

FIS Consent Management Solution

FIS Consent Management is designed to demonstrate compliance with key elements of the GDPR legislation. The audit-ready TruCert™ is a receipt for all consent interactions and data subject request interactions. The TruCert™ can also be used to record, at an individual level, non-consent grounds for processing data such as legitimate interest, ensuring that accidental processing does not occur. TruCert™s can be accessed via the Ledger/Notary API or directly by the customer through the "Data Rights" widget, which is included in the page.

Each TruCert™ is a digital certificate signed by FIS Consent Management private key using an RSA algorithm. This allows an immutable token to be created as a record of the consent and data rights interaction. FIS Consent Management analytics, available through the Enterprise Portal, can also be used to demonstrate the lawful basis of processing across the business and KPIs in delivering upon data subject requests.

Article 4, 7, 8: Articles relating to consent

Higher standards of consent are required by GDPR. **Article 4 (11)** specifies a consent must be active, represent affirmative action, present genuine choice and be time limited. Separate consents must be obtained for different processing activities or purposes. Forced or omnibus consent mechanisms will not be valid. Data subjects must have the right to revoke their consent at any time **Article 7 (3)** and it must be as simple to withdraw consent as it is to give it. In practice, at a minimum, this is likely to require organisations to allow consent to be withdrawn through the same media.

FIS Consent Management Solution

Gathering a separate consent for each purpose, whilst imposing a minimal imposition on the customer and ensuring high opt-in rates is a business-critical task. Success will be critical to a business's ability to harness data to drive superior customer outcomes and experiences. FIS Consent Management allows businesses to transform "consent" from a static, monolithic setting, towards dynamic, contextual customer interactions. The goal is to seek the right consent from each individual, at the right time and context.

Consent request widgets are integrated using java script tags into web applications. They can be triggered by context or using 1:1 targeting lists which are uploaded through a provisioning process and accessed via the context API. The actual consent widgets can appear inline or as an overlay (mounted in the page as a DIV or iframe). By using FIS Consent Management widgets, the DPO can ensure the consent notices are standardised across multiple touch points and the interaction will satisfy requirements for "clear" presentation. By the end of 2017, the DPO will also be able to control the notice provided to the customer via the FIS Consent Management Enterprise Portal, ensuring full control and minimising the chance of errors.

When FIS Consent Management certifies a consent that has been requested via a FIS Consent Management widget, it can confirm the exact notice that was presented to the customer within the TruCert consent receipt. FIS Consent Management then transforms the consent into machine readable data rights that can be accessed by business systems and platforms, via the rights API, to check whether lawful processing is possible. FIS Consent Management also calculates the durational (time limits) elements of a consent and expire the "data rights" at the appropriate time.

Article 6: Lawfulness of Processing

(Article 6) establishes that the right to process personal data must be lawful and establishes six categories of lawfulness. "Consent to the processing...for one or more specific purposes" is given primacy, but other lawful bases include:

- Performance of a contract
- Legal obligations
- Protection of the data subject's vital interests
- The performance of a task carried out in the public interest
- The purposes of the legitimate interests pursued by the controller or by a third party

The enterprise must be explicitly clear of the lawful basis of all personal data processing.

FIS Consent Management Solution

The lawful ability to process data is known as data rights within the FIS Consent Management platform. Beyond explicit consent management, FIS Consent Management also allows other lawful bases for processing to be notarised, at an individual level, and updated as circumstances evolve. This is achieved by populating the Method of Collection (MOC) and justification fields when invoking the API. For example, when a data subject enters a new service agreement, the business can notarise an array of data processing that will occur to achieve contract performance. Once the service is closed, the array of rights associated with the contract can be withdrawn. FIS Consent Management's restful APIs allow real-time access to up-to-date data rights, which means business systems and platforms can very easily access the "data rights" to process data.

Article 9: Processing of special categories of personal data

The GDPR has added protection for special, sensitive categories of personal data. **(Article 9)** states "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health a natural person's sex life or sexual orientation shall be prohibited, except where the data subject has given explicit consent to the processing of those personal data for one of more specified purposes."

FIS Consent Management Solution

FIS Consent Management enables express consent to be used to lawfully capture and process this sensitive data. Also, the consent & associated data types can be labelled as sensitive and therefore excluded from specific processing.

Article 15, 16, 17, 21: Right of Access, Rectification, Erasure and Object

The enhanced data subject rights give individuals the ability to review the accuracy of the data held by data controllers. A data subject has the right to **request access** to both the personal data and information on processing, recipients and data transfers **(Article 15)**.

Should inaccurate personal data about a data subject be held by the data controller, the data subject has the right to supply the correct information and request **rectification (Article 16)**. The inaccurate information should be updated *"without undue delay."*

Subject to certain conditions such as a data controller's obligation to comply with a legal obligation, a public interest obligation in relation to public health and in defense of a legal claim, a data subject can also request erasure of his or her personal data via the Right to Erasure ('the right to be forgotten') **(Article 17)**.

A data subject has the right to object **(Article 21)** to processing based on legitimate interest grounds or where necessary for a public interest task. The controller must then cease processing the personal data and the burden falls to the controller to prove why it should be able to continue to process the personal data.

FIS Consent Management Solution

FIS Consent Management provides several tools to assist the DPO to manage data subject rights. In particular, FIS Consent Management aims to assist in the customer, DPO and back-end system messaging associated with such requests. The tools include: specific data subject request widgets for embedding in web apps to provide a customer interface to lodge and review requests. Review and status monitoring within the DPO Enterprise portal and a message event service (launched in August 2017) that can pass data subject requests to back-end systems.

All requests and interactions are notarised in the TruCert™ digital certificates so the business can demonstrate to regulators and customers the interactions that have taken place.

FIS Consent Management also gives businesses the ability to act as the system of record for data location, but it is the business's responsibility to embed this data into API calls and act on the detail.

Importantly, FIS Consent Management isn't a privacy case management software application. If this deep level of functionality is required then additional technical suppliers will be required. Integration costs can be quoted upon request.

There will be four levels: request, triage, action and delivered.

Request

Businesses have two options for managing and recording data subject requests. They can create a website/app section that allows the customer to digitally lodge these requests on a universal basis or when referencing an individual data type that is processed by the business. The front end can either be rendered independently or a series of FIS Consent Management widgets (My Data, Data Subject Requests, My Requests) can be embedded into secure web pages to manage elements of the customer communication. Four types of requests are possible: Access, Erase, Rectify or Object. The object functionality can also be used to achieve the right to restriction of processing described in (**Article 18).**

Triage

During the provisioning process, businesses can configure whether a request should undergo triage review or automatic processing, according to the request type, the reason provided by customer or the data type. The DPO will view all the requests requiring triage within the FIS Consent Management Enterprise Portal. Once further review of the request has taken place (outside of FIS Consent Management platform) then the DPO can change the request status to "reject" or "accept". "Accept" decision will initiate the "actioning" phase. During this phase, customers can see request status, e.g., "reviewing" in the relevant widgets and an explanation of the process.

Actioning

During the "actioning" phase, a message will be passed from the FIS Consent Management Event Service (which was launched August 2017) to the businesses back-end system, such as an ESB or message queue, informing it of the customer request that must be actioned. From this point, it is the business' responsibility to enforce the request across the myriad platforms containing personal information.

Businesses also have the option to use FIS Consent Management to inform their back-end system of the location of data types affected by the customer request. This can be achieved if the business has inserted opaque data location information and pointers into API interactions with FIS Consent Management. The DPO will receive visual notification in the Enterprise Portal if delivery of a request is taking too long (against configurable SLAs). The ability to inform the customer of the late delivery of a request can be delivered by widgets and provide an explanation of the delay.

Complete

Once the business has completed the data subject request, the business' systems should provide a message to the FIS Consent Management Event System informing it of completion. Manual updates are also possible. The status of the request will subsequently update within the Enterprise Portal and the MyRequests widget.

Access requests must be compiled and delivered to the customer, outside of FIS Consent Management, to minimise personal data disclosures and enhanced risks. But it is possible to notarise the delivery of download links and erasure notices, as well as the actual data download, using the Notary API.

Article 20: Data Portability

The right to data portability **(Article 20)** allows a data subject to request the personal data they've supplied to a controller be shared with another data controller in "a structured, commonly used and machine-readable format".

FIS Consent Management Solution

FIS Consent Management currently caters for the consent associated with data sharing to be captured in a certificate, but it is the business's responsibility to share the consent data with the recipient and deliver the underlying data.

Conclusion

GDPR compliance may require significant changes to business processes, customer interactions and technical platforms. Whilst there could be a temptation to attempt compliance by tinkering with existing platforms, achieving a wholesale improvement to managing customer data rights at an individual level across the business will generally require a new platform. Indeed, businesses operating in the EU are given the mandate by GDPR to ensure their data protection efforts are achieved "with due regards to the state of the art"; they should carefully consider whether truly empowering individuals requires the use of a consent and data rights platform like FIS Consent Management.

Abstract

The EU GDPR regulation, which will be enforced on 25 May 2018, revolutionises the data privacy landscape in Europe. GPDR gives individuals greater control and transparency over their personal data and raises the bar for businesses to achieve lawful processing of personal information. Achieving compliance will require more than technical solutions, as it will be necessary for businesses to strategically shift their data focus to recognise individual rights. However, this white paper outlines how, using the FIS Consent Management platform, businesses can simply and quickly solve eleven key articles of the incoming regulation, avoid heavy fines and sanctions as well as empowering customers with enhanced, personalised services.

About FIS

FIS is a global leader in financial services technology, with a focus on retail and institutional banking, payments, asset and wealth management, risk and compliance, consulting and outsourcing solutions. Through the depth and breadth of our solutions portfolio, global capabilities and domain expertise, FIS serves more than 20,000 clients in over 130 countries. Headquartered in Jacksonville, Florida, FIS employs more than 56,000 people worldwide and holds leadership positions in payment processing, financial software and banking solutions. Providing software, services and outsourcing of the technology that empowers the financial world, FIS is a Fortune 500 company and is a member of Standard & Poor's 500® Index. For more information about FIS, visit **www.fisglobal.com**

Contact us:

Telephone: +44.(0).1923.471.850
or email us at: **getinfo@fisglobal.com**
bonita.osgood.fisglobal.com