iGrant.io
Your data, your choice.

Between the Business and the Customer: Managing Consent in a Data Sharing Economy

The Role and Influence of a DPO

September 2018

Contents

Growing Consumer Awareness

Two months after the introduction of the General Data Protection Regulation (GDPR), a survey carried out by SAS, a leading data analytics company[1], showed that a significant number of UK and Irish consumers were activating their new personal data rights, and faster than expected.

The report which covered almost 2,000 consumers found that over a quarter of those surveyed had already exercised their GDPR rights over personal data and more than half plan to do so within the next year significantly more than the number a year before[2].

This swift response shows the level consumers value and are aware of their data privacy rights under the GDPR. Organizations need to be ready for these customer data requests as it is increasingly clear that organizations that treat their customers' data with care will be the ones rewarded. The ones that don't will not only face fines but the loss of reputation and potentially customers, as well.

Just as the GDPR was coming into effect, the Facebook/ Cambridge Analytica data misuse story increased awareness and interest in data privacy. 76% of UK and Irish survey participants who were aware of the Facebook/Cambridge Analytica story have either activated their GDPR rights or at least re-assessed the information they share and how organizations use it.

According to the survey, consumers view the handling of personal information as an issue of trust and have a low tolerance for data mistakes or misuse, such as having their data shared with third parties without their consent. Almost half of participants said they would activate their data rights after only one mistake. Nearly one-third of participants said that if an organization had misused their data, they would withdraw their permission to use it entirely, regardless of any assurances, offers of improved services or financial incentives.

1 https://www.prnewswire.com/news-releases/sas-survey-a-quarter-of-uk-and-ireland-consumers-have-already-exercised-gdpr-rights-300691660.html. The research was commission by SAS and conducted by research company 3GEM. Between May and June 2018, 1,000 consumers in the UK and 850 consumers in the Republic of Ireland were surveyed.

2 https://www.sas.com/en_gb/news/press-releases/2017/july/uk-adults-polled-intend-to-activate-new-personal-data-rights.html

However, respecting data privacy and consent shows that companies can win back customers that promise they will not share data with third parties or misuse their data.

It's not surprising that young adults have a more open attitude toward sharing personal information than their elders with nearly half saying they are less likely to erase their data with a company as long as they are assured it will not be shared without consent. Young people are also much less likely to activate their data rights if they can receive a satisfactory incentive. For example, young people are willing to exchange data permission for financial rewards, free merchandise or more personalized services than older age groups who are far less willing to accept those trade-offs.

Not all industries have been equally affected by GDPR. In particular, social media companies and retailers are more likely to be targeted by customers wishing to erase their data or to have it withdrawn from being used for marketing purposes.

More transparent data management and analytics are crucial, not only to achieve compliance but to provide personalized customer experiences that make consumers more willing to share their data. Ensuring that businesses do not fail to respect their customers' data - and thereby risk losing competitive advantage which in turn hurts the bottom line - is the prime responsibility of the data protection officer.

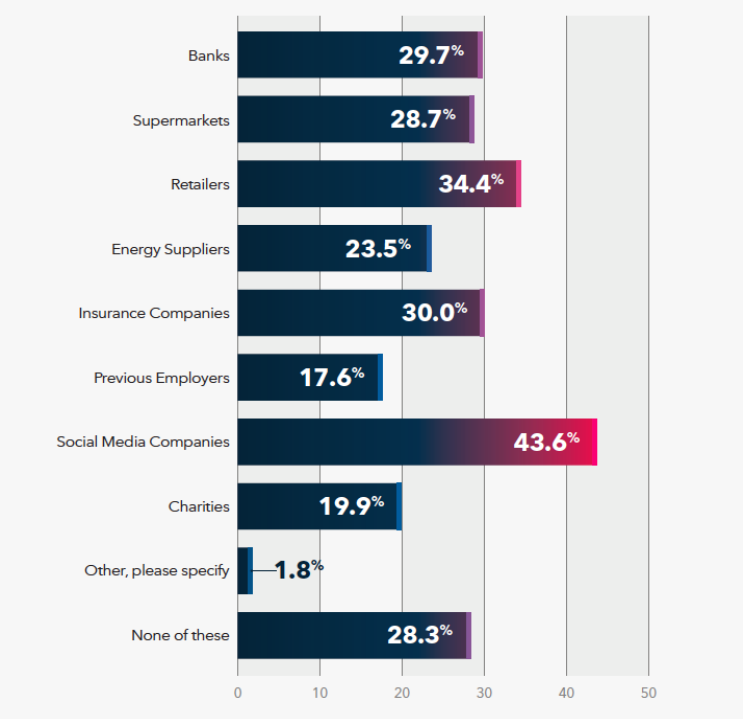

Figure 1: From which of the following organisations have you exercised/will you exercise your right to have your data removed?

Who Needs A DPO?

Most organisations that collect, store or process large amounts of personal data about EU citizens, whether employees, individuals outside the organization – or both – are mandated under Article 37 of the GDPR to have a data protection officer (DPO).

DPOs must be:

> *appointed for all public authorities, and where the core activities of the controller or the processor involve 'regular and systematic monitoring of data subjects on a large scale' or where the entity conducts large-scale processing of 'special categories of personal data*[3]*.*

The DPO is an enterprise security leader with responsibility for overseeing data protection strategy and implementation to ensure compliance with the requirements of GDPR and other applicable data protection regulations.

DPOs are responsible for ensuring that company employees are educated on important compliance requirements, and that there are staff trained in data processing and conducting regular security audits. DPOs serve as the point of contact between the company and any Supervisory Authorities (SAs) that oversee activities related to data.

The DPO's tasks are delineated in Article 39 of the GDPR to include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, training data processing staff, and conducting internal audits.
- Advising with regard to data protection impact assessments when required under Article 35.
- Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.

3 'Special categories of personal data' include details of race or ethnicity or religious beliefs

- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

These responsibilities mirror those of privacy professionals elsewhere around the globe and signal a growth spurt for the profession, although evidence suggests that many firms will outsource DPO responsibilities to specialized agencies or law firms. A company with multiple subsidiaries (a “group of undertakings”) may appoint a single DPO who should be “easily accessible from each establishment.” The GDPR also allows the DPO functions to be performed by either an employee of the controller or processor or by a third party service provider, creating opportunities for consulting and legal firms to offer outside DPO services.

Under the GDPR, DPOs have many rights in addition to their responsibilities. They may insist upon company resources to fulfil their job functions and for their own ongoing training. They must have access to the company’s data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line “to the highest management level” of the company. DPOs are expressly granted significant independence in their job functions and may perform other tasks and duties provided they do not create conflicts of interest. Job security is another perk; the GDPR expressly prevents dismissal or penalty of the DPO for performance of their tasks and places no limitation on the length of this tenure.

In short, the DPO has the authority to drive positive outcomes for the business by shaping the relationship between the company its employees and customers.

GDPR Compliance & Consequences

- Know what data you need to hold and why
- Understand why you need to process this data in the context of a specified purpose.
- Document what data you will process. Determine how your organization will acquire and revoke individuals' consent to share information. Create a policy to document this process.
- Recognize the rights granted to individuals through GDPR, including rights to specific groups like minors.
- Compare your existing procedures to GDPR requirements and make edits where required to meet identified gaps.

Becoming GDPR compliant starts with understanding the new requirements and determining what business processes are impacted from the policy changes. There are six steps to help you evaluate the GDPR's impact on your organization.

In addition, Articles 13 and 14 of the GDPR impose an obligation on controllers to provide a significant amount of information to data subjects about the processing of their personal data, stating specifically that the information provided to data subjects about the processing of their personal data must be given in a concise, transparent, intelligible and easily accessible form. The GDPR leaves controllers with some discretion in terms of the manner in which fair processing information is communicated to data subjects. It also gives the controllers the opportunity to choose the mechanics through which they meet its transparency requirements.

Commercial Benefits

Effective fair processing information is likely to have a number of commercial benefits:

- Data subjects are more likely to place trust in organisations that are transparent about the use of personal data. This trust will contribute to customer loyalty and retention.
- Data subjects will be likely to provide more and more valuable personal data to organisations that will use it properly.
- The risk of complaints and disputes arising from the use of personal data will be reduced when the processing undertaken by an organisation is explained to the data subject.[4]

4 Hannah Jackson, CIPP/E, IAPP

The Conundrum

Of all the requirements and expectations, the most demanding challenge facing DPOs is the balancing act between protecting corporate interests and customer (regulatory) rights. It's not surprising that many DPOs are lawyers or have a legal background. It make sense for companies which may face severe penalties in cases of data mismanagement violations: a lawyer may be better equipped to better protect and defend the company in such cases than a non-law educated professional.

Prioritising a company's interest over consumer rights is an approach that is, sooner or later, going to come unstuck. As the introduction to this paper demonstrates, the pendulum has swung very much in favour of citizens' rights. The only corporate strategy that resonates today is one which engages with the core privacy principles underpinning the GDPR that can both respect consumer rights and provide a competitive advantage. The key is to build a long term trust relationship with customers that is predicated on keeping them informed through transparency and an ongoing dialogue.

Project Fear

But, if you think that the role of the DPO is a fearsome project associated with raising the company drawbridge against the 'gotchas' of the GDPR, it doesn't have to be. Although many may perceive the job as one for a dull administrator or a bureaucratic policeman, it doesn't take a great leap of faith to realise that it can be so much more than that Really!

Building better customer relationships is the cornerstone of every successful business and one of the key players in achieving that is the person who controls the levers at the company-customer interface. That is, the DPO. DPOs have the authority to drive positive outcomes for the business by creating trusted relationships with clients, by protecting their consumer rights and enabling them to partner in the management of their personal data. In other words, the DPO has a really important role in the company, a role that adds value and not only avoids penalties

iGrant.io Solutions

iGrant.io[5] provides consent management products and services for organisations and individuals. Data sharing consent agreements are complex, often requiring real-time access to several partners. The iGrant.io privacy-preserving SaaS-based platform provides solutions that facilitate regulatory compliance for all types of organisations and offers businesses and users ease of access and use.

The iGrant.io API is easy to adopt and integrate into an organisation's IT environment. Consumers sign consent agreements on the organisation's website or via the iGrant.io mobile app. One of the benefits of the API is that iGrant.io only maintains a record of the transaction. Even for a peer-to-peer consent agreement, no personal data is exchanged or shared with iGrant.io, ensuring that the services provided are not intrusive, either for the companies making consent requests or for their customers. The collection, storage and processing of personal data is the organisation's responsibility as agreed with its customers.

The iGrant.io mobile app is available on iOS and Android. For organisations, there is an initial fee for installation/ subscription (including support) with a subsequent transaction-based business model.

How iGrant.io Benefits:

(A) Businesses

From a company perspective, the impact of consumer rights under the GDPR can be distilled down to seven key areas which are listed at Annex B.

(B) Consumers

The ways in which iGrant.io addresses the eight key consumer rights are listed at Annex C.

iGrant.io and the GDPR

iGrant.io is designed to be an invaluable aid for companies and their customers to collaborate on the sharing, management and storage of personal data. It is a tool that enables DPO's to address the initial GDPR data sharing with customers and also allow them to take the next step to creating a trustful relationship. Customers can collaborate with the DPO in how to share and manage the storage of their personal data, ensuring compliance with the GDPR and its underlying principles as well as with other data protection regulations.

iGrant.io's functional alignment with the GDPR is listed at Annex A.

5 iGrant.io is wholly owned by LCubed AB

How iGrant.io Helps The DPO

iGrant.io manages consent requests by providing:

- the means to handle right to forget notifications
- immutable consent logs for any customer which would be valid in a court of law, if the need arose
- a good view of all data attributes used by the company and the purposes they are put to
- the ability to directly mark whether any given attribute is sensitive or not; and marking any sensitive information by default as DISALLOW
- the opportunity to share data with partners and other third parties beyond the company's lawful business use
- the insights to clean data that is surplus to company requirements

At first sight, achieving and maintaining compliance with the GDPR – or any other data protection regulation – appears to be a daunting prospect. As we have shown, the way to overcome these concerns is to turn the new regulatory landscape into a competitive business advantage by engaging in a positive way with customers to create a win-win. The building block of this win-win approach is an environment of transparency and trust, which is where partnering with iGrant.io is invaluable.

iGrant.io provides a consent mediation platform and service that enables reliable, trustworthy and regulatory compliant data sharing between any organisation and their users – healthcare providers and their patients, financial services companies and their customers, airlines and their passengers. iGrant.io is non-intrusive, and does not touch any personal data.

The iGrant.io mobile app provides a single point of access to all the organisations with which consumers have a data relationship. It provides a holistic and granular view of how, where and when the consumer's data is being used. The iGrant.io cloud-based service provides reassurance that companies are in step with what their customers expect from them. It offers the security of knowing that iGrant.io is tracking and maintaining a record of each exchange and transaction concerning their use of customer data.

iGrant.io offers a DPO the ability to better manage customer data access consent requests (see sidebar).

In this new GDPR environment iGrant.io is a partner who can provide the tools the DPO requires to enable them to build a long-term relationship with employees and customers as well as senior management and the regulatory authorities. iGrant.io solves these challenges and we look forward to demonstrating all the benefits of this data sharing eco-system to all its stakeholders!

Annex A: iGrant.io and GDPR

Article 5: Principles relating to processing of personal data

iGrant.io provides:

- a platform on which companies can provide information on what personal data they store, process etc. It also provides an end-user app for viewing this.
- companies with consent information for any individual. iGrant.io stores and processes only the consent attributes. However, as iGrant.io does not store any personal data, companies are responsible for compliance issues relating to data storage.
- a real time consent interface to end users where they can set their preferences on how to control their personal data.
- an interface that companies can continuously update. It also provides information on what data is present, and, if a company allows, it also displays the information.
- End users are able to update their consent information in real- time. iGrant.io also provides a notification to companies if the end user changes their consent and, if a company allows, it provides a notification for correction/ veracity. iGrant.io can visually inform the user if their data is being accessed and used by the organisation

Article 6: Lawfulness of processing

iGrant.io provides data subjects with an interface to mark their consent for the use of their data for purposes other than for legal reasons. Companies can retrieve this information via Restful APIs.

Companies are allowed to add the purposes they see needed for their business which either require or do not require consent

Articles 6.2 – 6.4 are not applicable to iGrant.io.

Article 7: Conditions for consent

iGrant.io holds consent information history and provides a report to businesses.

iGrant.io provides an interface for data subjects to allow/ disallow consent in real-time at the attribute level. The platform allows companies to upload a simple JSON file on what the information is going to be used for within the organisation.

The iGrant.io mobile app or web portal allows data subjects to mark their decisions dynamically as well. The company gets a detailed report on, firstly, the latest consent values at attribute level, as well as the consent value at any historic time

iGrant.io enables end users to set consent rules for their data. Your data, your choice

Article 8: Conditions applicable to child's consent in relation to information society services

iGrant.io provides an interface to the legal guardian of under age children. iGrant.io can be automatically configured for age limits according to the applicable legal jurisdiction. iGrant.io will have a validation process to ensure real users.

Article 9: Processing of special categories of personal data

iGrant.io defaults personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation to disallow by default. iGrant.io does not store any organisation's personal data, it only stores the consent data.

iGrant.io will default certain purposes as not modifiable depending on a country's jurisdiction.

Both Article 10 (Processing of personal data relating to criminal convictions and offences) and Article 11 (Processing which does not require identification) are not in the scope of iGrant.io, being the responsibility of the organisation.

Annex B: iGrant.io Business Benefits

Below are the key features relating to the storage and processing of personal data your customers will expect under the GDPR:

Lawful basis of processing

You need to have a legal reason to use customer data which could be consent (they opted in) with notice (you told them what they were opting into), performance of a contract (e.g. they're your customer and you want to send them a bill), or what the GDPR calls "legitimate interest" (e.g. they're a customer, and you want to send them products related to what they currently have). You need the ability to track that reason (also known as "lawful basis") for a given contact.

Consent

One type of lawful basis of processing is consent with proper notice. In order for customers to grant consent under the GDPR, a few things need to happen. They need to be told what they're opting into and to affirmatively opt-in: filling in a form alone cannot implicitly opt them into your company's data usage requests. The purpose for which consent is being requested also needs to be granular, covering the various ways your personal data is being used.

Deletion

Customers have the right to request that you delete all the personal data you have about them. In such a case, the GDPR requires the permanent removal of all personal information from your databases, including email tracking history, call records, form submissions and more. In many cases, you'll need to respond to their request within 30 days

Withdrawal of consent

Customers need the ability (as the data subject) to see what they're signed up for, and withdraw their consent (or object to how you're processing their data) at any time. In other words, withdrawing consent needs to be just as easy as giving it.

Access / Portability

Customers can request access to the personal data you hold about them. If they request access, you (as the controller) need to provide a copy of the data, usually in machine-readable format (e.g. CSV or XLS). They can also request to see and verify the lawfulness of processing (see above).

Modification

In addition to a request to delete or access their data, customers can ask your company to modify their data if inaccurate or incomplete.

Security Measures

Some form of adequate data protection safeguards (e.g. encryption at rest and in transit, access controls, data anonymization) have to be provided.

iGrant.io supports all the above requirements through its platform and the provision of self-service for individuals to opt-in/opt-out of sharing their data at the attribute level for declared purposes which are also configurable.

Annex C: iGrant.io Consumer Benefits

The right to be informed

Organisations need to tell individuals what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language.

iGrant.io's default solution is to provide a platform to make consumer data visible and for a given purpose.

The right to access

Individuals can submit subject access requests, which oblige organisations to provide a copy of any personal data concerning the individual. Organisations have one month to produce this information, although there are exceptions for requests that are manifestly unfounded, repetitive or excessive.

iGrant.io's self-service system provides this as a default function. The individual can merely subscribe and view their personal data, what they are used for and control it

The right to rectification

If the individual discovers that the information an organisation holds on them is inaccurate or incomplete, they can request that it be updated. As with the right to access, organisations have one month to do this, and the same exceptions apply.

Where an organisation is capable of federating with iGrant.io, the solution connects to the organisation's IAM system to fetch the information, which is part of iGrant.io's data quality feature.

The right to erasure

(also known as 'the right to be forgotten')

Individuals can request that organisations erase their data in certain circumstances, such as when the data is no longer necessary, the data was unlawfully processed or it no longer meets the lawful ground for which it was collected. This includes instances where the individual withdraws consent.

iGrant.io provides an option to request to an organisation's DPO who is notified and alerted about each individual's request

The right to restrict processing

Individuals can request that organisations to restrict processing Individuals can request that organisations limit the way an organisation uses personal data.
It's an alternative to requesting the erasure of data, and might be used when the individual contests the accuracy of their personal data or when the individual no longer needs the information but the organisation requires it to establish, exercise or defend a legal claim.

iGrant.io's platform provides the function to disallow the use of their attributes for a given purpose. A future release will provide the functionality to lock that information (patent pending)

The right to data portability

Individuals are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that an individual has provided to data controllers by way of a contract or consent

iGrant.io provides a data sharing option to upload and save personal data with a particular organisation.

The right to object

Individuals can object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority. Organisations must stop processing information unless they can demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual or if the processing is for the establishment or exercise of defence of legal claims.

iGrant.io provides a detailed view of what information is being used for what purposes. In cases where individuals are not satisfied apart from locking/ disabling that information, they are able to alert the DPO

Rights related to automated decision making including profiling

The GDPR includes provisions for decisions made with no human involvement, such as profiling, which uses personal data to make calculated assumptions about individuals. There are strict rules about this kind of processing, and individuals are permitted to challenge and request a review of the processing if they believe the rules aren't being followed.

iGrant.io provides a detailed view of what information is being used for what purposes. In cases where individual are not satisfied apart from locking/disabling that information, they are able to alert the DPO.

iGrant.io is a cloud-based personal data and consent mediation platform that enables a fully transparent and trustable data sharing economy.

It helps institutions, both private and public, unlock the value of personal data in compliance with, for example, the General Data Protection Regulation. Apart from lowering the cost of legal compliance, iGrant.io helps companies establish and maintain trust with their customers by demonstrating transparency and respect in how personal data is used.

Bössvägen 28 Sollentuna
192 55, Sweden

info@igrant.io
www.igrant.io