GDPR Overview

In April 2016, the General Data Protection Regulation (GDPR) — a joint proposal by the European Commission, European Parliament, and the Council of the EU which provides individuals with even greater control over the collection and use of their personal data- was adopted by the European Union.

As a provider of a world-class Exhibitor Manual, which by its nature has a global reach and deals with the processing of email contact and engagement information, XPOBAY is committed to ensuring our customers are able to comply with their requirements under the GDPR.

With that goal in mind, we've created a robust privacy program that integrates data privacy into XPOBAY's software. Among other things, the key steps that we are taking to comply with the GDPR regulations are:

- Documented all data processing activities that involve the collection, treatment, and safeguarding of personal data
- Built new processes and features to ensure we can quickly and effectively address any requests from our customers when their subscribers wish to exercise their rights (including the Right of Access, Right to Rectification, Right to Object, Right to be Forgotten, and the Right of Portability)
- Reevaluated all of our sub-processors to ensure they have adequate security measures in place for the safeguarding of personal data processed by them and ensuring our contracts with them require them to also abide by their requirements as sub-processors under the GDPR

Consent and Purpose

While the definition of 'personal data' under the GDPR is largely unchanged from its predecessor, the EU Directive, the inclusion of reference to "online identifiers" is potentially a major shift for marketers' perception of the data they hold and how it should be handled. So, if you're storing data about a person in a usable way, it probably relates to some identifier of a natural person (including online identifiers like device IDs, cookie IDs, etc) and is, as a result, personal data.

Personal Data must be "Processed lawfully, fairly and in a transparent manner"[2]

Consent and Transparency

For all data covered by the above definition of personal data, you'll need to be able to justify that you're processing it lawfully. Consent is just one way of establishing that your processing activities are the GDPR, but it is likely going to be the one most applicable to the email marketer. Just as it has been with email marketing in the past, explicit, purpose-based collection, that is freely given is the highest standard for data collection and use policies. This means that there is no ambiguity as to the activities consented to or the organisation carrying out those activities.

Consent should be clear and unique to a specific organisation and each reason for processing. Methods like separate forms or separate, default unchecked boxes are obvious options. While there may be other, more creative options that are equally viable, it is important to ensure that clarity is not lost in the process. The transparency of your reasons for processing data is a requirement for building explicit consent. As always, data subjects should be able to withdraw their consent for each, or all, processing activity, and withdrawing consent should be as easy as giving it was.
As with all GDPR-related things, records keeping is vital to demonstrating compliance. Make sure that, however you decide to do this, these records support your consent-based legal grounds.

Security

Risk and Appropriate Technical and Organisational Measures

While personal data is defined very broadly under the GDPR, the sensitivity of the data and the severity of harm that may result in the event of unauthorized access to the data, is not equal. This means that the measures by which you secure personal data (type of encryption, backup procedures, password requirements, etc.) may vary by data type and the processing activities undertaken using that data. The GDPR requires protection of personal data using "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" throughout the life cycle of the data.

The regulation does not prescribe any specific security mechanisms, but rather requires that data controllers and processors take into "account the state of the art,

the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons"6 should data be subject to accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access.

Some measures that the GDPR highlights are pseudonymisation and encryption, but the extent to which they represent a standard for data security is unclear. Until more clear guidance is released from the EU, we recommend keeping an eye out for guidance from industry thought leaders, trade organisations, and data security experts and organisations (like the National Institute of Standards and Technology, or NIST), but there may also be clarity in Member State laws and future documents issued from the EU governing body.

Regardless of your current security measures, the GDPR highlights the need for ongoing evaluation of risk to personal data and security measures based on product evolution.

Privacy By Design

The GDPR's "Data Protection by Design and by Default" model, or more commonly, 'privacy-by-design' model, requires that principles of data protection should be taken into account at the product development phase rather than after data is being processed. By implementing appropriate technical and organisational measures, taking into account the nature and sensitivity of data types that will be processed, and ensuring that appropriate data minimization measures are implemented at the product (and feature) development phase, personal data is protected at all stages of its life cycle.

Data Breaches

If you're getting a hint of that new-regulation smell, that's because data breach handling and notification is a previously-untouched scope of data privacy law in the EU. In the GDPR, rules for how and when you should notify data subjects and/or relevant authorities are made more clear.

Notice from Controllers to Supervisory Authority:
For controllers, notice to the appropriate supervisory authority must be made "without undue delay and, where feasible, not later than 72 hours" after becoming aware of the breach with the following information:

1. Describe the nature of the personal data breach including where possible,
    1. The categories and approximate number of data subjects concerned; and
    2. The categories and approximate number of personal data records concerned
2. Include the name and contact details of the data protection officer or other contact from whom more information may be obtained
3. Describe the likely consequences of the breach
4. Describe what the controller is doing to address the breach and/or mitigate possible adverse effects.

Throughout the process of identifying, measuring the scope of, and remediating the effects of the breach, records should be maintained to "enable the supervisory authority to verify compliance with this Article."

Notice from Processors to Controllers:
Processors must inform "the controller without undue delay after becoming aware of a personal data breach".

Notice from Controller directly to Data Subject:
If the personal data in question represents "high risk to the rights and freedoms of natural persons," the controller will need to notify the data subject without undue delay. This notification should include a description of the breach in clear, plain language that includes contact details for the appropriate person (DPO or otherwise), the likely consequences of the breach, and the current and future measures the controller will take to address the breach.

There are a few exceptions to the data subject notice requirement: where the controller employed safeguards or has taken subsequent action to render the risk of the breach inert, and where individual data subject outreach would require disproportionate effort. But as with any exception under the regulation, legal counsel should be sought before proceeding.

How can I submit a request to exercise my (or my subscriber's) GDPR rights?

1. Contact security@xpobay.com
2. Ensure that your email subject is "GDPR Request", and mention the appropriate subcategory of Deletion, Retrieval, or Rectification to indicate the specific GDPR rights you'd like to exercise.
3. Please provide the following information in the notes with your request (this part is important for us to be able to help as quickly and accurately as possible!):
    1. Full name of data subject, email address of data subject, username for account, admin email address of the account, Name of client account
4. Our Support team will be in touch with confirmation that we've received your request, and we'll start processing for you as quickly as possible. You'll receive confirmation when we're all done and we'll make sure to deliver any collateral in a secure format (if applicable).

If your subscriber's personal data was provided to us in connection with any prior request for support or services, please indicate this when submitting the request to our Support team.