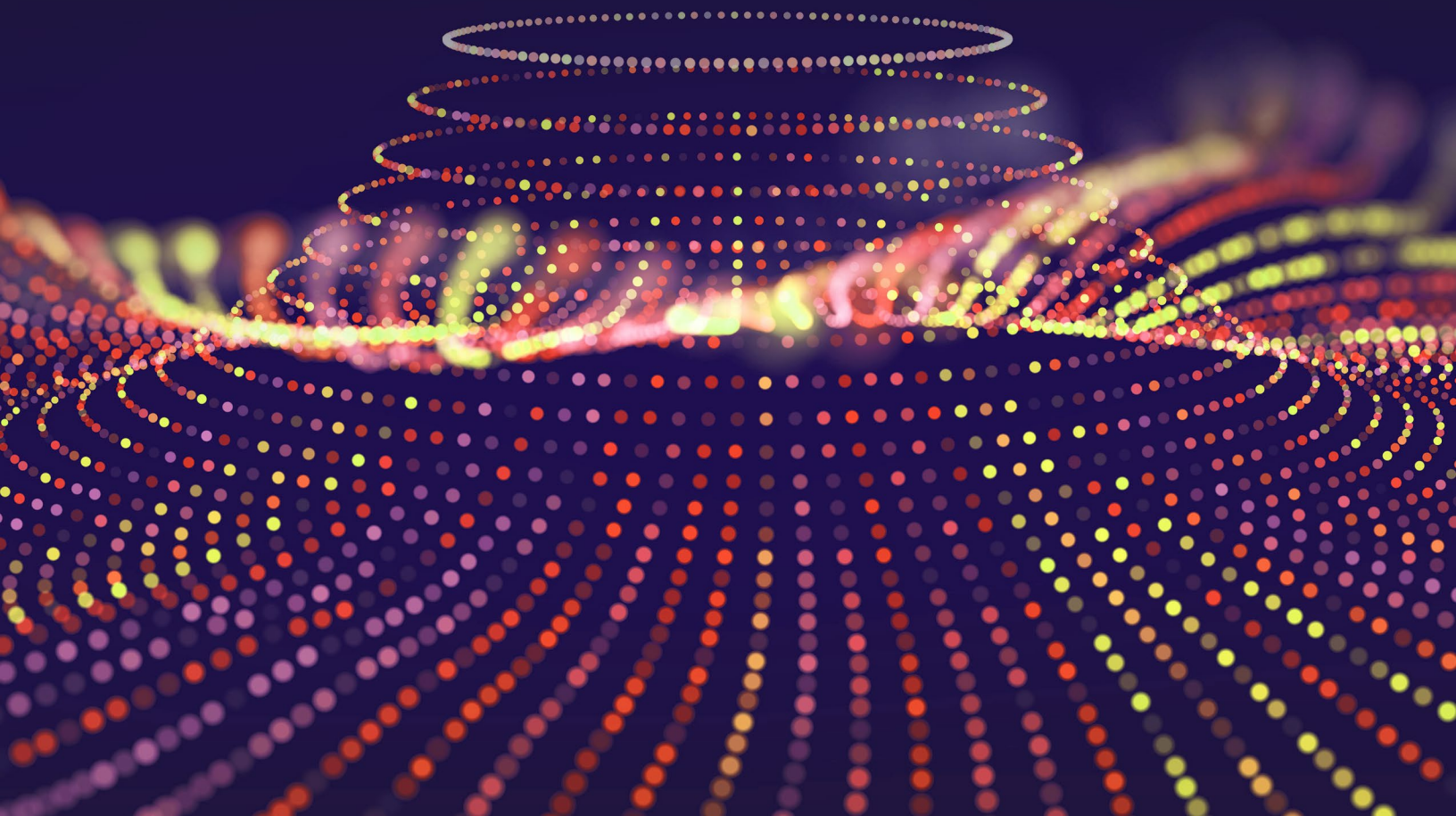
EXPONEA
EXPERIENCE CLOUD

WE KNOW

GDPR



GDPR
without stress

Ways GDPR impacts your business

GDPR will fortify your customer relationships -
if you play it right

You don't have to lose the game deleting your entire emailing database (just in case) in a panic fit, just like J.D. Wetherspoon did just to prevent possible damages.

By neatly spring cleaning your data, you will know where to reach: which data you hold, for what purpose, whether it is legitimate and as to whether or not you transfer it in an inadequate way, or store it longer than you would need. Knowing your data, especially knowing whether the specific purposes are covered by consent, and having a good tool is key for controllers to master the situation around GDPR.

The awareness of each of your data processing activity will give you the needed leverage over your competitors who would rather bin the data instead of ordering and reusing it wisely.

How (not) knowing the data subject rights impacts your business

Under the new legislation, companies and cloud-software providers won't be able to get away with just stating "By using this site, you accept cookies" anymore.

Without an explicit affirmation from your users, your business simply doesn't have the consent to use any user data for marketing purposes. This includes the data you already have.

How well do you know your data? And why does it pay off to know the data subject rights?

Don’t make a €20 mil mistake...

If a threat of a possible admin fine coming up to €20 million or 4% of your global turnover (whichever is higher), doesn’t sound scary enough, maybe you shouldn’t ignore the possible damage of your business reputation. Any damage resulting from non-compliance can make your business appear as unsafe for your customers’ data in the digital marketplace.

In order to be able to keep processing your user data aligned with the new rules of GDPR, it is crucial to learn what their actual rights are. This will help you find ways to respect the rights without damaging your business and improve your users’ browsing experience at the same time. It is a win-win. Just keep reading...

The right to be informed

Data subjects have the right to be provided with information on

a) the identity of the controller
b) the reasons for processing their personal data and
c) other relevant information necessary to ensure the fair and transparent processing of personal data.

A good tool will help to map your data

To ensure you abide by this rule, you have to map your data. Where does your customer data flow and how is it processed? **You should now be able to explain clearly on your website:**

This way you will not only be in control of your data, and ensure you are compliant, but you will also take a clever step to keeping your users.

If your email database doesn't comply yet, you will simply get consent again. Exponea can A/B test different scenarios and figure out more effective ways of getting that consent. By personalizing, automating and A/B testing the marketing communication will effectively preserve your existing, momentarily non-compliant, database.

With the right tool you can think beyond the requirements of GDPR and take all marketing goals, as well as your own goals, into consideration.

Exponea on best consent getting ideas

Now, here is a chance to shine. There are many ways to get your website visitors' consent without scaring them off. So how can you play around with the slickest consent getting ideas until they are tailored to perfection?

The secret is to present the information in the cookie as beneficial to the customers as it gets; making them feel secure, informed and happy to consent. Be upfront with your customers about using their data, where and for how long it will be stored. Be clear about how exactly the customer benefits from their data collection.

Here is just one example of a notice (web-layer, cookie notice) that pops up within 5-10 seconds after the user enters our webpage for the first time:

> *"We are happy you are here. Help us understand what your preferences are by enabling cookies so we can help you find relevant information as soon as possible. Should you not enable them, you may still use our website. However, we can't improve and tailor your browsing experience based on your interests or location."*

You can also add a non-invasive formulation offering both consent and opt-out button:

“Yes, customize my browsing experience” and “No, thanks.”
(Alternatively: “No,don’t optimize my browsing experience”)

The right of access

Part of the expanded rights of data subjects outlined by GDPR is the right for data subjects to obtain from the data controller confirmation as to

a) whether or not personal data concerning them is being processed,
b) where, and
c) for what purpose.

Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

This change is a dramatic shift to data transparency and empowerment of data subjects.

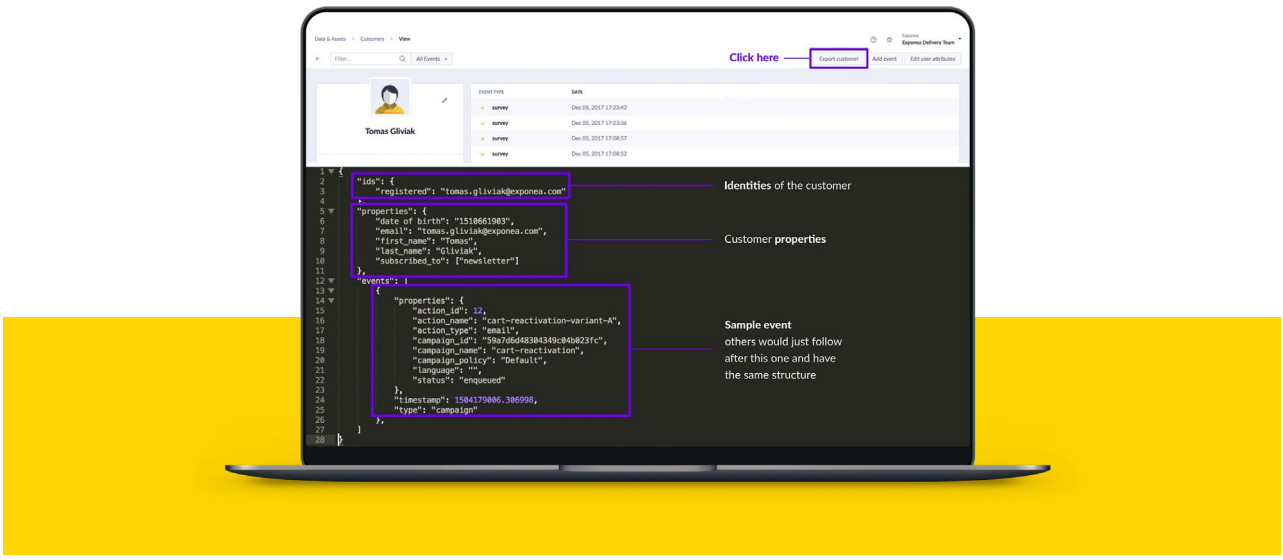
Exponea holds your data in one place

Exponea customer profile means that you already have all the information about the customer in one place, which makes providing data a piece of cake.

If you have all the data in Exponea, you can refer to data mapping to double-check if you are compliant.

Exponea additionally allows you to download customer data using data API in JSON format, which is easily transferable.

We can export data, move them and explain the purpose - make them easily accessible and be able to explain what is what.



This way you can use and share your GDPR compliant and tidy database ad hoc for any client that would enquire about it. You might also be able to export the GDPR compliant data from it.
The added value in this is that the GDPR compliant database is usable and exportable elsewhere, with no risk of getting a hefty fine.

The right to rectification

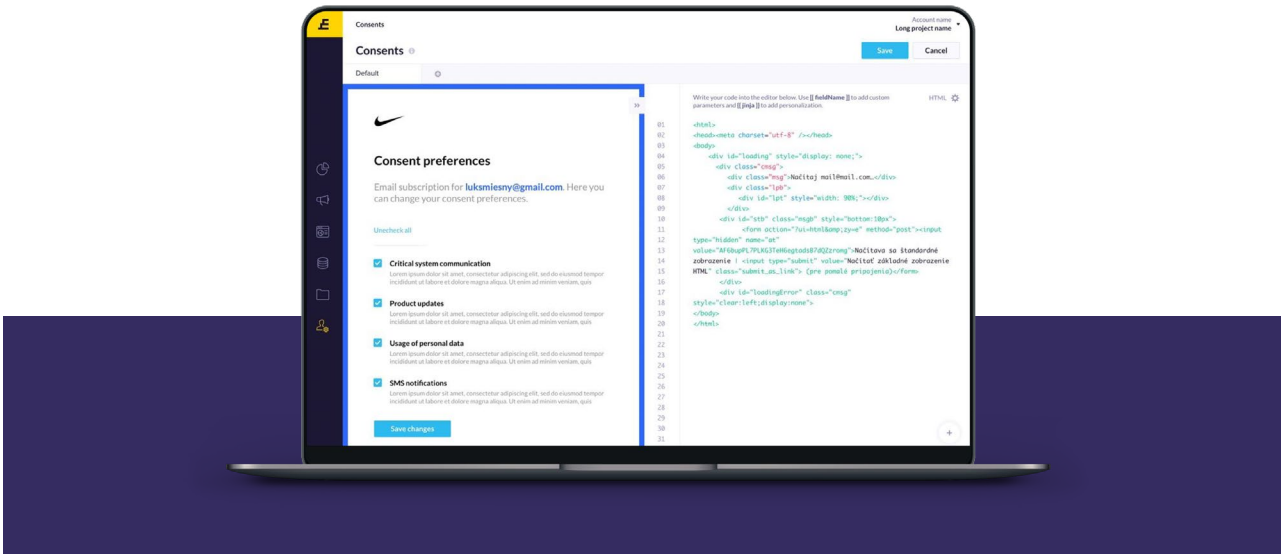
Controllers must ensure that inaccurate or incomplete data is erased or rectified.

Data subjects have the right to rectification of inaccurate personal data.

Exponea enables you to amend data

To make your customer service ready to handle hundreds of manual rectification requests, you can ensure the users are easily able to change inaccurate or incomplete data in their profile.

You can easily update existing data inside Exponea from a profile page, or a freshly prepared landing page for managing consents.



The right to erasure

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Delete data without losing track

Apart from being able to delete customers from Exponea using Data API, you can automate data deletion across all platforms by using scenarios and webhooks.

Since you will be deleting all data, even events, you may lose historical trends and revenue data, which makes it hard for you to do meaningful YoY comparisons and analysis Anonymization of data would allow you to still see aggregate metrics, as events would be assigned to a new random cookie and personal information would be deleted. If you publish any private data that can be, for example, looked up using Google or any search engine, the right to erasure gives you additional obligations. If in this case user requests erasure of data is made public, you have to undertake "reasonable steps" to inform other controllers, processing the data in question, about this.

The right to restrict processing

Data subjects have the right to restrict the processing of personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:

a) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy);
b) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure);
c) the controller no longer needs the data for their original purpose, but the

data is still required by the controller to establish, exercise or defend legal rights; or if

d) verification of overriding grounds is pending, in the context of an erasure request.

Flag the restricted data

In case this happens, the data has to be removed from the filing system or from a public website in order to avoid further processing.

You will be able to flag the questioned data in a way that it is clear the processing has been constrained, from certain timestamp. No additional data will be processed without re gaining consent or fulfilling other legitimate basis for processing.

The right to data portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a ‘commonly use and machine

readable format' and have the right to transmit that data to another controller.

Solve it with a ready template

Data subjects can now ask whether we possess their personal data and what kind of data. They can ask for copies or have it transferred to a competitor in a portable format (JSON). Exponea uses JSON (Java Script Object Notation), a lightweight data-interchange programme.

If this happens, you can have a template response email ready. If your customer service team knows how to respond, they might even leverage the situation and re-establish the relationship with leaving customers.

Perhaps offering them a perk or reminding them of some added value created by your service to them, you can make them stay - and boost the mutual interaction.

The right to object

Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data, where the basis for that processing is either of public interest; or legitimate interests of the controller.

It is about plain language disclosures

Controllers have to disclose how long the data will be stored and inform data subjects of the right to withdraw consent at any time, request access, rectify or object to processing, or lodge a complaint with a supervisory authority, according to article 13.

The disclosures have to be easy to access and written in plain language adjusted to the audience. Hence, statements designated to children have to be formulated in a way they can understand.

When designing our disclosure, we have to make sure the statement is readable and watch out for very long sentences, passive voice, adverbs and hidden verbs.

You don't need to ask for consent in order to process the user's order. However, you should ask whether you may use personal information for anything else. If there are more purposes you may use the information for, you have to ask for permission separately.

YOU CAN OFFER YOUR USERS A SIMILAR NOTICE:

How will we use the information about you?

Personalize your use of the website (if you agree).

Rights in relation to automated decision making and profiling

Data subjects have the right not to be subject to a decision based solely on automated processing which significantly affect them (including profiling). Such processing is permitted where it is necessary for entering into a contract with the data subject. This all provided that it is authorized by law, or that the data subject has explicitly consented and appropriate safeguards are in place.

In other words, To make data processing fair, it has to be done in a transparent manner,

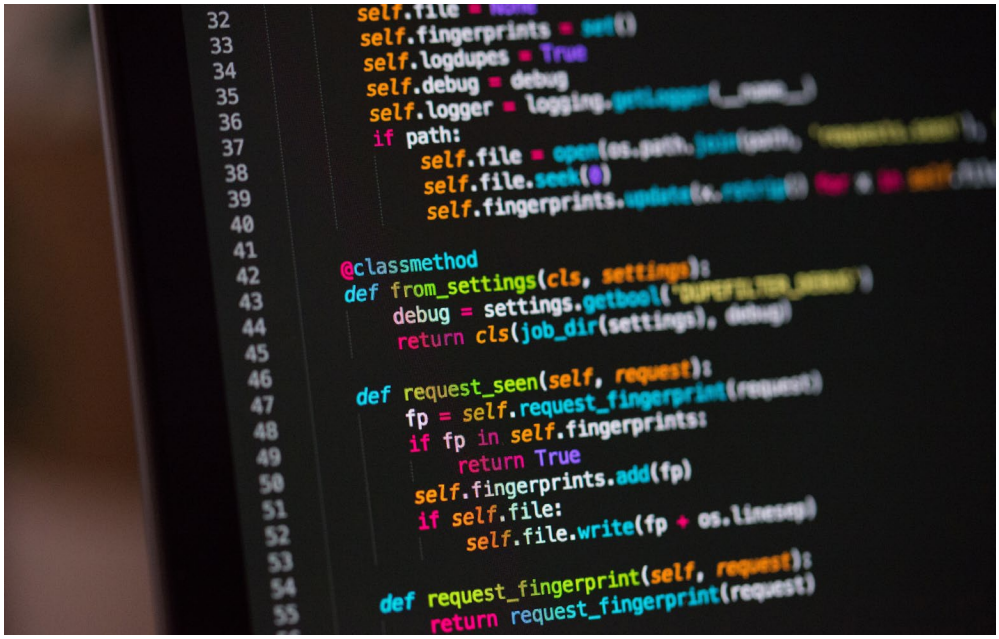
ensuring the users are informed about the purposes of the processing, the existence of profiling and its consequences.

The users should know the consequences of their actions, should they decide against providing the data.

How to prepare your email marketing for GDPR

What should you do to be ready
and safe from harm?

Exponea worked out **seven tips** that would help any affected e-commerce, regardless of the size.



Start using hashes for communication between 3rd party providers

Are you using one vendor for sending and evaluating a customer satisfaction survey, and another one to deliver it to your customers? Establish a new ID, for example use SHA-256 hashing algorithm from your lower-cased emails, and let vendors exchange data this way. Only you hold the key which pairs the real email to a hashed ID.

Exponea lets you set up multiple IDs to empower you in this decision. You can still automatically pair customers based on the new ID, but make sure that you renew your data policy agreement with your vendors to keep your customers informed, should they wish to review it any time.

Dig up your consent data, if you do not use it now

Sometimes, when you had been transferring data from an older to a newer solution, you did not import columns which you did not consider important. Just a subscription and an opted-out-flag was usually enough.

Dig through your old automation tool data (e.g. Mailchimp, Mailgun) for an opt-in timestamp, IP and so on, which can be used as a basis for your customers' consents.

Exponea lets you additionally import any historical data or data from other systems to existing customers, so you will be able to fill in the consents, if you had not had them in Exponea yet.

Analyze current and future campaigns

Find out whether you have asked the customer for their consent for every purpose. Think ahead and ask for a consent for future use cases, instead of relying on your general existing consent, e.g. a consent you obtained from your user just to use an email as a channel.

Can you use all the data you have collected in a new use case? If it is a yes, because your previously gained consent allows that - happy days.

Targeted campaigns to regain consent

Establish purposes of collecting and processing data and start thinking about the reactivation campaign. Engaged users are more likely to give you their continuous consent, but what about the non-engaged?

Your subscriber count will probably lower at first, but engagement rates will go up, as you

are keeping engaged customers, with their explicit consent.

Do you know what else goes hand in hand with this? Deliverability and inbox placement increases. Why? You are now targeting only engaged people and receiving domains will notice: your spam complaint rates or straight delete rates, which come into play, will get significantly lower with the engaged audience.

Exponea helps you to use previous purchase, browsing or email data to personalize the subject line or the content, and make your creative content even more powerful.

By undertaking Subject-line experiments Exponea can test the best ways for getting consent and revamp our communication with clients. Also, maybe it is worth mentioning that getting consent via SMS has a high open rate.

Update your opt-out policies and establish consent groups

Allow your subscribers to opt-out as easily as it was to opt-in. The ideal situation is one landing page in their profile, which allows the customers to exercise their GDPR rights: data deletion, anonymization, or just the option to unsubscribe from a daily newsletter should ideally be in one place.

Use this place to emphasize the benefits of keeping the data: you can emphasize what the customer could get as a subscriber - that they would not get normally.

In Exponea you can use the custom consent page in Exponea's Privacy Tutorial to manage this portal. Likewise, you can use Data API to build your own and send relevant data to Exponea.

Allow subscribers to take a one-month vacation from your emails, using a simple scenario in Exponea.

Clean up your emailing database

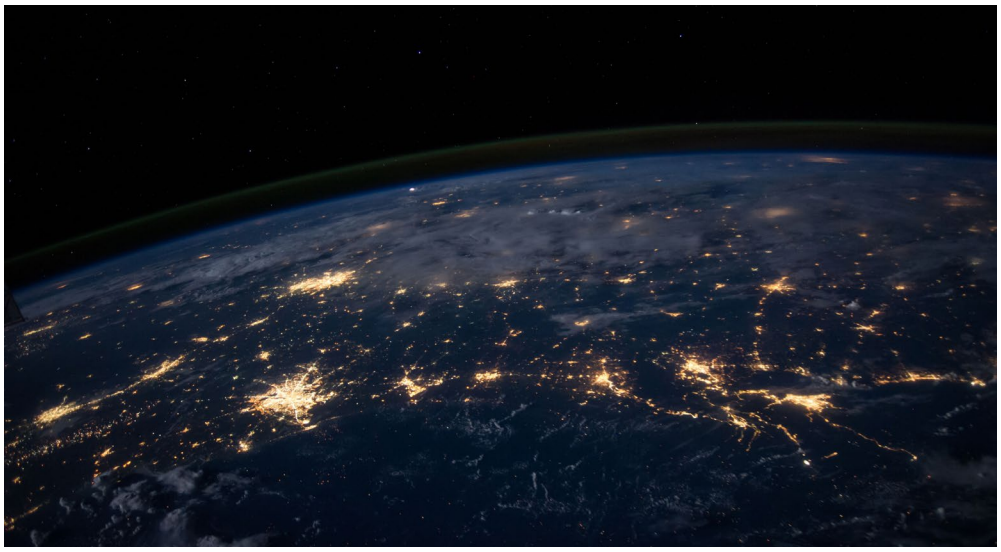
In order to do the spring-cleaning in your database, you can start with the following action points. Make sure that you are:

- Using email as the main, unique ID
- Pairing customers based on other ID, coming from your CRM, e-commerce solution or internal SQL database
- Aware of all duplicate emails

Regarding the duplicate emails, it is eminent to be aware of the consequences of one unsubscribed “profile”, where the customer receives an email next day anyway - due to her other existing profile... Do you think the customer would care that you have had duplicate records? Can you pinpoint customers with session and purchases, who never open their email?

Maybe next time your customers appear on the site, it would make sense to ask them via a web layer, whether email would the best channel to contact them through.

To make things easier, Exponea can help you with automatic deduplication of emails, apart from reports showing you who the duplicates are.



Map your data

Before anything else, the best advice on hand would be an actionable checklist. Make sure you tick the following boxes and you have the answers ready.

You should know...

- the way your data flows between different processors
- where your databases are
- your weak points from the security point of view
- for how long do you keep customer data
- your data retention policies and you also identified their impact on the long-term user cases and programs

FAQ
about GDPR

Most of Exponea's clients come from e-commerce, predominantly from the fashion industry, but any business in the digital marketplace can find an analogue in the frequently asked questions we gathered for you here.

Will we need new consent from all existing customers?

In general, Yes. Unless you were already collecting a GDPR compliant consent.

What does it mean? If you had gained it with a standard business practice (e.g. such as pre-ticked box, non-trivial wording, aggregation of consent) you will most likely need a new consent to cover all the intended operations with your customer data.

However, if you're unable to gain new consents and your already collected consents are of good quality (e.g. understandable, confirmed by further action), you can at least use them to send non-personalized emails with noncurated content. Exponea enables you to do so very simply.

Do we need to do a double opt-in?

Most likely not. Double opt-in is neither regulated nor specified by GDPR, but by existing local regulations concerning advertising. Its role, however, serves as a basis for the legitimacy of the database and the demonstration of the customer consent.

Do we need to name some of the channels that we will address in the future?

Generally yes, but here you have to define the concept of a channel because there is no such term in GDPR. This definition must be clear and concrete for the user.

When getting a consent, it is the purpose for the consent we need to define, rather than the communication channel we use.

We have to ask the user if we can send a newsletter - if the answer is yes, it is ok to send it

via different channels such as SMS, post or email.

Think about it like this: you can have many marketing channels used for one or different purposes. It's a matter of definition.

Now, as each purpose requires consent, it brings us back to the consent: what defines correct consent, which is the best consent?

It is one clearly defined consent that gets you all. You can ask the users to help you improve your omni-channel communication with their consent - and include all the channels in the answer.

How will I be able to transfer consents to Exponea? What if I am collecting them via multiple channels and from different sources?

The data API, which we released at the end of February, is a response to the many questions referring to data exchange. In addition to API, it is still possible to track custom event "consent" through JS SDK to Exponea, directly from the web.

You can then set up consents and parameters of consent within Exponea. Data API allows you to have centralized flow of data to Exponea from various systems, with the ability to switch read/write permissions for different data types.

It also serves the purpose of easily complying to a customer request, whether it is a data download, anonymization or portability.

Do we need to give our customers the ability to opt out from individual communication channels? How and where?

Yes, you should give the customer options, as granular as possible without flooding them with too many choices creating a decision paralysis.

Opting out should be easy - the same way as it was to opt in.

You can create a single consent page located on your website and link from every communication channel.

To sum it up, the customer should be able to get to that setting in a simple way.

Third parties: How to solve enumeration? For example, in case of RTB house which combines banner placements from hundreds of individual websites?

In your company's privacy policy, it is necessary to provide information to the affected customers specifying why their data is being collected and with which third parties it is shared.

However, again, from your users you only need consent for each purpose of the data processing. You don't need a consent for each added third party explicitly.

Your users give their consent to different types of communication on your marketing channels, which you have to define in your privacy policy, because GDPR does not know the term "channel".

It is important to always inform the users about where their data goes, or whether it is used outside of the EU. It is just about transparency. The user has the right to erase the data or

have it corrected.

E.g. You use one marketing automation tool as a third party and you want to change it for another, or add a new automation tool. You should inform the users about this in your privacy policy by changing the information, but once you have the consent from the user to send them an email, you can go ahead without asking them for a new consent - the purpose of their email in your hands namely did not change.

On what grounds can we use “legitimate interest”?

A legitimate interest is only for specific circumstances related to the customer - for example, a transactional email is something related to delivery.

The definition of a legitimate interest is not black and white, and you have to consider the specific situations where the customer’s interest is “probably” justified and when it is definitely not.

If we send an email saying - “Your order is on the way” - it is related to the customer’s legitimate interest of getting their purchased order.

Here the business interest is more inclined to the customer - it is basically in the customer’s interest to get their ordered item.

However, it is in your legitimate interest to offer the customer new items or send them a voucher (even if you want to offer them a discount).

In the registration process, the customer has the opportunity to sign up through his Facebook profile - do we still need a special permission to send marketing information?

Yes, you do. By signing in only with Facebook, your customers will not give you a transparent consent.

How will it be with the phone/SMS/email order - if the customer does not register, do we have to record the call/order? How long will we store it in this case and do we have to report it somewhere?

Here we are talking about transactional communication that falls within the area of legitimate interest. You need to register your order information. However, the creation of an order does not give you consent to any data processing other than the transaction.

GDPR
more than ready

Exponea makes the best effort to hold your hand through the adaptation process, keeping you informed.

By knowing the rules and finding parallels in the solutions of your marketing peers', you will certainly benefit from the best practices instead of losing clients while stumbling through the seemingly scary change of play.

If you did not find all the answers, there is a good summary of rather basic rules (such as Who does GDPR apply to?) here.

Establishing yourself as a safe harbor for your customers' data can be something you can use as a new way of communicating and doing business with them. Something to be seen definitely as an opportunity, not a disadvantage.

At Exponea we understand the risks and the opportunities. We will guide you step by step through the transformation and walk you out of the risks without a headache.

Contact us if you have any further questions concerning getting GDPR ready.

Glossary

Data subject

a living individual to whom personal data relates, the person whose personal data are collected, held or processed.

DPIA

Data Protection Impact Assessment, a procedure that has been designed to help organizations identify, assess and mitigate (or minimize) data privacy risks - it is a direct consequence of the accountability principle of GDPR.

DPO

Data Protection Officer. Ensures that the organization processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the data protection rules.

ISO 27001 certification

A specification for an Information Security Management System (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

ISO 9001 certification

Quality Management System (QMS) is internationally recognized as the world's leading quality management standard and has been implemented by over one million organizations in over 170 countries globally.


EXPONEA
EXPERIENCE CLOUD