PUSHPUSH GO

Mylo law & tax

24 CHANGES THAT GDPR WILL INTRODUCE IN YOUR MARKETING STRATEGY

and why they do not apply to web push notifications

TABLE OF CONTENTS

INTRODUCTION

If you've heard of **GDPR**, you probably read that it will be a "**revolution in the subject of personal data**" or even "**death for marketers**".

There is more and more information about the GDPR online, the majority of which is not very specific, stressing how many new obligations and penalties these regulations will introduce. This regulations can sometimes be difficult to understand and you can make hasty conclusions without diving deep into the subject. That is why, to familiarize ourselves with this topic, for **marketers from the European Union**, we have invited experts who solve complex legal problems in simple ways.

We have created this guide together with the law office MyLo, which, like us, follows the principle that "nothing is impossible".

FROM THIS ARTICLE YOU WILL LEARN:

- how some current popular marketing practices will have to change **after May 25, 2018**,
- why **web push notifications are effective, and at the same time "GDPR-friendly"**, because they do not involve the processing of customers' personal data.

Enjoy!

Joanna Worotyńska
VP of Communication and Marketing @ PushPushGo

Agnieszka Grzesiek - Kasperczyk
Legal Advisor, Partner at MyLo law office

WHAT: GDPR, or the EU General Data Protection Regulation

FROM WHEN: in the European Union, May 25th, 2018

MAIN CHANGES:

- data minimization, meaning data is processed to the smallest degree needed to achieve the business goals,
- in the content of the consent agreement, you do not need to cite any legal acts, article numbers or journal numbers,
- the obligation to ensure that the consent to the processing of data can be as easily withdrawn as has been given,
- the "privacy by default" principle,
- "the right to be forgotten",
- an obligation to inform users about the transfer of personal data outside of the European Union, e.g. through the MailChimp or OneSignal platforms,
- use of automatic actions (profiling-based), which lead to the display offers of the same product to different people, but with a different prices, will be prohibited.

CHANGE OF YOUR APPROACH

GDPR requires a change of approach to personal data. Data about clients and leads is a valuable asset. Treat them as if this is not your money.

First of all, the GDPR requires a change of approach to the protection of personal data. You can no longer treat this matter "neglectfully". Personal data protection has to be included everywhere "by default". Therefore, you have to **respect privacy by default**. You can only interfere with it if it is **allowed by law or with the consent of a specific person**.

We live in an era in which data has become an asset more valuable than money. The point of the GDPR directives is that the processing of personal data should be **secure, transparent, trustworthy and in accordance with the will of the person who entrusted it to you**.

Joanna Worotyńska
VP of Communication and Marketing @ PushPushGo

Since the topic of GDPR has become a real challenge for UE marketers, many PushPushGo clients, before starting any business talks, ask me if they **can implement a web push strategy without worrying about the changes that these regulations will introduce**. No wonder, given the not-so-precise "cautions" that appear on the subject in public opinion.

Thanks to these developments, every marketer or business owner will know how to adapt their current activities to the new requirements. What's more, it is a good opportunity to emphasize that **web push notifications are one of the marketing channels that the GDPR does not apply to**. This is due to the fact that this technology is not based on the processing personal data - it does not use email or IP addresses and cookies.

The subscriber remains anonymous throughout the communication process. Nevertheless, the data we have about them gained through the web browser allow **precise targeting** on the basis of behaviors on the website as well as clicks on given products.

NO GUIDANCE, BUT COMPLIANCE WITH THE LAW IS OBLIGATORY

GDPR is expected to achieve data security and respect for privacy.
It does not give you any tips on how to achieve this.
Every company must choose the right tools for itself.

The previous law on the protection of personal data gave quite **specific guidelines** on what to do to be in compliance with the law.

Let us assume that there is a marketing department in a company, and this department **sends subscribers a newsletter**. According to the old law, in such situation you were to:

- obtain and archive all consents given by the subscriber, so that there was no doubt who signed up for the newsletter and who didn't,
- create a security policy, i.e. a document describing all the rules governing how personal data was processed in the company,
- create an IT system management instruction, i.e. a document describing how each user should use computers owned by the company; what anti-virus programs were used, the rules of granting access rights to personal data, etc.

When GDPR comes into force, these obligations will disappear (except the one regarding consent, which will be discussed in a moment).

You should still have internal documentation that describes all the rules for the proper processing of personal data. However, **GDPR does not say anything about what this documentation should look like**.
Each company should adapt its own procedures and policies to its own needs, to the scale on which it processes personal data. It is clear that these processes look different in a small online store than they do in a company that runs a social networking site.

However, the GDPR requires both companies to ensure the same level of data security, and that their data processing is legal (only on the basis indicated in the regulations). This is possible only by establishing appropriate **internal rules** and ongoing monitoring to ensure that these rules are followed. These rules should concern both IT security and current work on documents containing personal data (paper correspondence, employee documentation, contracts concluded with clients in paper form, invoices, etc.).

YOUR CUSTOMER = YOU CAN PROCESS PERSONAL DATA FOR MARKETING PURPOSES

According to GDPR, you do not need to obtain special consent for the processing of your clients' data for marketing purposes.
This does not mean, however, that you can do anything with this data.

You can find a lot information online saying that after GDPR comes into force, practically **all processes involving the use of personal data for marketing purposes will require consent**. That's not true.

In accordance with GDPR, the current principle remains that the basis for processing personal data may also be the "**legally justified interest**" of the administrator. According to GDPR, you can process personal data if:

- it is necessary to ensure IT security (eg. backing up),
- you make direct marketing of your own products and services,
- data processing is necessary to perform the contract or communication before its conclusion (response to the customer's request).

You do not need to place check-boxes regarding consent to the processing of personal data "for contact" under the contact forms on your website.

It is also not necessary to include clauses that the client consents to the processing of his personal data "in order to execute the contract".

People who are your clients would not even have to give consent to the processing of their personal data "for marketing purposes".

The consent to send commercial information via email is required by another act, i.e. the act on the provision of electronic services. This is the prohibition against sending SPAM. Your marketing mailings will not be considered "junk" only if you have previously obtained explicit consent to send them to a specific person. The same **applies to text messages**, in which case the requirement to obtain separate consent results from the Telecommunications Law. SMS campaigns and so-called cold calling can be used only in relation to those who have previously agreed to it.

However, this is a different type of consent than consent to personal data processing. So let's not confuse concepts and do not place all the blame on GDPR. In addition, one check-box or click is always less than two check-kboxes.

BE CAREFUL, THE PRINCIPLE OF DATA MINIMIZATION APPLIES

> *Do not process data longer than it's needed.*
>
> *Do not collect "on stock" data. Just ask for the data that is really necessary.*

GDPR puts a lot of emphasis on the principle of **data minimization**, data processing to the smallest degree that is needed to achieve the desired business goals. Minimization is to concern both the scope of collected (and further processed) data as well as the processing time.

If you have already acquired any personal data - whether these are your customers or people interested in your offer - **it does not mean that you can store this data "forever"** and that you can do anything with it.

This is important for you as a marketer. Minimizing data firstly means that you should - colloquially speaking - **"clean" your marketing base regularly**. From the point of view of GDPR, it makes no sense to store details about people you know will most likely not use your offer anymore or will be unlikely to contact you about a previously sold product or service.

So, coming back to the principle that "you can process personal data of your customers for your own marketing purposes", it's important to remember that this is not always the case. You should - based on your marketing practices and their results so far - set some time after which you consider the particular type of data to be useless. From the point of view of GDPR, it will be necessary to establish **an internal procedure according to which you will delete unnecessary data**.

Second, the principle of minimization means that **you should not accumulate too much data**. Consider what customer data you really need for marketing, based on the tools you actually use. Do not collect information "on stock". Just "because once a phone number may be useful" approach -- will not be compliant with the GDPR rules.

YOU MUST INFORM USERS ABOUT THE RIGHT TO OBJECT TO THE PROCESSING OF DATA FOR MARKETING PURPOSES

You must inform users about the right to object to the processing of data for marketing purposes at the first stage of your communication.

We indicated above that in relation to your existing clients you can conduct marketing activities without additional consent for processing data (you only need permission for mailing or other forms of communication, e.g. text messaging).

However, in order to act in accordance with GDPR, **you must inform people that they may object to such processing at any time.**

This should happen "at the first stage of communication" with the client.

If it was a newsletter, information about the right to opt out should take place at the subscription section. When it comes to marketing to existing customers, this information can be presented at the stage of contract conclusion (in the form of a linked privacy policy, for example) or immediately after the transaction (on the thank you page).

DO NOT COLLECT TOO MUCH INFORMATION AT ONCE

Collect only the data that is necessary for the purpose that you communicate to the customer.
Do not collect and keep personal data "on stock."

As we have indicated above, the GDPR puts a lot of emphasis on the principle of data minimization. You should not collect information that is not needed for the purpose for which the user provides you with data.

Example: if you offer an e-book, then you do not need the phone number of the subscriber to send this e-book, nor data on which company he works in, his position, or his name and surname. The only personal data you need to send a free e-book is an email address.

We understand that as a marketer you probably want to **have as much information as possible about a given lead immediately**. However, GDPR indicates that this is not the way to operate. You should not "extort" information from the user under the guise of a different purpose than you actually have.

Of course, you can offer an e-book as a gift in exchange for subscribing to a newsletter.

However, **GDPR requires transparency**. If this is your goal (acquiring the subscriber in exchange for free content), you should not write: "Do you want to receive an e-book?" And underneath place a form with mandatory fields to fill in: email address, telephone number, company data, first name and last name.

Instead, write: "In exchange for subscribing to our newsletter you will receive a fantastic e-book". In this case, one box to fill in an email address is enough. You can also ask for a name, although this should not be an obligatory field.

NEWSLETTER, LEAD GENERATION, PHONE NUMBER COLLECTION - FIRST GET THE PERMISSION

If you generate leads, you need to have really clear consent regarding the processing of personal data.

If your consent was not 100% correct in the past, you will have to collect it again.

As mentioned before, in regards to your existing or former clients, you do not have to focus so much on their consent to the processing of their personal data.

However, the issue of acquiring new contacts from people who are not currently your clients is completely different. If you collect email leads, newsletter subscribers, or a list of people who are willing to receive text messages from you, **you must obtain their consent**. The GDPR requires that consent to be **voluntary**, **specific**, **conscious** and **unambiguous**. Four adjectives and you'll see that each of them is associated with the specific responsibilities of the marketer.

This means that you need to take a good look at your current lead acquisition methods. For example, if you used Facebook Lead Ads, but you were convinced that it is a completely legal tool (after all, Facebook offers collecting contacts in this way, so they had to ensure appropriate consents from users) - it may turn out that on the basis of GDPR, you will not be able to use these leads.

GDPR does not introduce a general rule that after May 25th, 2018 you must "refresh" all your previous consents. It also does not require sending out mass mailing on this day (which would significantly burden all servers in the European Union!)

The GDPR requirement, however, is that **you should prove that you have the appropriate consent from people who are in your database.** If you have not taken care of such "material evidence" before, unfortunately your database will lose its value altogether. You will have to obtain their consent again.

Joanna Worotyńska
VP of Communication and Marketing @ PushPushGo

Web push is the first marketing channel **absolutely based on the principle of permission marketing**. This means that subscribers consciously agree to your notifications and can resign from them at any time through their browser.

There is no question of adding the written recipient to the subscription list again, which can happen, for example, in email marketing.

The result is that **web push marketers are more cautious** in what, to whom and how often they send. Such a subscriber is simply a lot easier to lose. Additionally, directly you can check when someone subscribed to your notification, right in the panel.

VOLUNTARY CONSENT

Consent must be voluntary. Do not make the agreement conditional upon consenting to the processing of personal data that is not necessary for the performance of the contract.

Offering a gift (lead magnet) in exchange for providing personal data for a specific purpose (like subscription to a newsletter) is allowed. GDPR does not change in this matter. Remember, however, that the subscriber must be properly informed and aware of the purpose for which the data is supplied.

The GDPR lists several features that should define consent, received from any person, concerning the processing of personal data.

The first of these is **the consent is voluntary**. You can not make the conclusion or performance of the contract conditional on consenting to the processing of data that is not necessary for the performance of this contract (because you do not need consent for the processing of data for the performance of the contract - see page 5).

For example if you sell kitchen furniture, you can not make the transaction (the sale of a set of furniture) conditional upon the customer's consent to transfer his personal data to a company from the household appliances sector in order to choose the right set of kitchen equipment for you.

There is no problem if you offer a gift (e-book, video recording) or voucher in exchange for signing up to a mailing list. You only need to clearly specify what data you are asking for, what the purpose is and what you offer in return.

GDPR indicates that in some situations there is an imbalance between the parties and then the request of the "stronger" entity for the subject's "weaker" consent to the processing of personal data may not be perceived as truly giving a voluntary choice.

An example, think of an employer who asks employees for permission to be monitored at the workplace. It is obvious that the employees' decision on this issue may be dictated by the fear of losing their job if they do not agree. Such consent will therefore not be seen as voluntary in the light of the GDPR.

SPECIFIC CONSENT

Consent must be specific.

Use clear, simple language to state exactly you are asking for (what data), for what purpose and who will use the data.

The GDPR also indicates that consent must be specific. What does this mean? There are several conditions:

- the user needs to know who is receiving the consent. You should provide your details in the consent statement. If you intend to provide data to third parties, they should also be mentioned in the consent. The wording "and partners" is not enough,
- the user must know what exactly he or she is agreeing to. It is best to indicate which data we are talking about (only email address, or postal address, telephone number, purchase history, etc.),
- the user needs to know for what purpose they are giving you the data. If you intend to process data for several purposes, it would be best to prepare a separate agreement for each purpose. Sometimes it may be acceptable to collect several goals in one agreement if they are closely related to each other.

Correct agreement content:
I agree to the processing of my personal data given above (name and email address) for XYZ for marketing purposes.

Incorrect agreement content:
I agree to the processing of my personal data in accordance with the regulation of the European Parliament and Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free flow of such data (EU OJ No. L / 119/1) for administrative, statistical and marketing purposes by the owner of the portal and its partners.

What is incorrect in the example above?

- The entity that will process the data is not given (only the "owner of the portal" is indicated, but no one knows who it is);
- It is not indicated which personal data this consent refers to;
- Mysterious "partners" were indicated -- an unspecified group of entities;
- Several processing purposes are given at the same time, it is not known what "administrative purposes" mean. It would be better to use only the term "marketing goals", because statistical purposes fall into the former one.
- The GDPR title is unnecessarily specified. It only obscures the content of consent and makes it difficult to read. The content of the consent does not require any legal acts, article numbers or journal numbers.

CONSCIOUS CONSENT

The consent must be conscious - the **specific positive action of the user is required**.

Using checkboxes that are selected by default does not count as consent.

GDPR requires that the process of collecting consent must be carefully designed. Regulations indicate that, for example, overly **intrusive checkboxes** that disrupt service may not be considered as conscious consent. Someone who gives this kind of consent will not act in a fully conscious and voluntary way.

It is also worth coming back to the question of the Facebook Lead Ads tool. GDPR does not require that you stop using it, but you should ensure that check-boxes are in the last step before submitting the form. By using these checkboxes, the user will deliberately agree to provide his or her personal data to you.

The "basic" mechanism of Facebook Lead Ads, which automatically fills out the form with personal data of the user, will not be accepted in the light of the GDPR.

> *Consent must be conscious.*
>
> *Active user action is required. Silence can never be considered as consent.*

CLEAR CONSENT

> *Consent must be unambiguous.*
>
> *You can not presume consent from another behavior, such as accepting the regulations or joining a webinar.*

GDPR also requires that consent be unambiguous. The point is that **it can be inferred from a given user's behavior that he gave consent.**

Yes, that's right - from "behavior." So consent does not always have to be a "text". It does not have to be a checkbox. The mere provision of an email address may be considered as consent to the use of this data for the purpose of sending a newsletter - **if you construct the form properly.**

A request for consent may also appear as a pop-up window on the site or notification. If the text on this pop-up or notification is properly worded, the same click can be considered as consent.

As we have already pointed out before, you cannot, by the fact that someone has registered on the webinar or downloaded the e-book, conclude that they have also agreed to receive commercial information (maybe they just wanted to participate in this one webinar?). Such a record or download of an e-book i**s not synonymous with a subscription to the mailing list.**

Also, be careful with placing the content of consent agreements in the regulations or other longer texts that the user has access to. Acceptance of "terms & conditions" is not tantamount to agreeing to add an email address to the newsletter or other marketing database.

Sometimes consent can be expressed implicitly. The given behavior must be so unambiguous, specific and conscious that it constitutes obvious consent to the processing of personal data, despite the fact that it will not contain any written or oral statement.

As an example, you can indicate handing a business card or throwing it in a container from which the prize draw takes place, like at an industry conference. The sharing of a business card is tantamount to giving consent to the processing of data contained therein for business purposes. However, this should not be understood as a consent to the addition to the general marketing database and, for example, to send this person mass sms.

CONSENT MUST BE EASY TO WITHDRAW

Consent must be easy to withdraw.

A deactivation link that was previously a good practice is now a duty.

GDPR imposes a new obligation on consent collected from users. It's always been a **good marketing practice** but now it will be **a legal requirement**. We are talking about the obligation to ensure that consent can be as easily withdrawn as it was given.

What does this obligation mean in practice? The easiest way to do it is to enable users to inform you about the withdrawal of consent **through the same communication channel in which the consent was granted.** For example, remember to include the phone number at which users can revoke their consent on your website. If you have obtained consent for email correspondence, provide a deactivation link at the bottom of each email message. Remember that small, barely visible fonts are insufficient. **The link to unsubscribe should be clear and visible.**

The right to withdraw consent should be made known to the user at the moment of receiving consent. It can be a simple phrase like "Remember that you can always opt-out by clicking here."

Joanna Worotyńska
VP of Communication and Marketing @ PushPushGo

The subscriber can withdraw consent for receiving web push notifications in 3 different ways:

- **At any time - in the settings section in your browser,**
- **At any moment - through widgets that you can additionally enable on your website, like the inbox or the subscription bell.**
- **Immediately after dispatch - clicking on the gear icon in your notification.**

Make sure your audience knows about it before they start with your web push activities. This will increase their confidence in you and, consequently, increase the subscription rate.

BE CAREFUL, METADATA ANALYSIS MAY REQUIRE SEPARATE CONSENT

> *Write exactly what data you will process. Do not conceal anything.*

If you have already received marketing consent from previous users and you want to be in compliance with GDPR, think about whether the consent that you have from users actually corresponds to the processes that you then performed on the data of those users.

Most likely, you use not only data given to you by customers (name, email address), but also **the history of their email opens, purchase histories and other data you have about them (gender, age, location preferences, etc.)** when sending marketing emails.

According to GDPR, personal data is any information about a specific person, including details like knowledge about their behavior or preferences. Therefore, if you want to implement marketing campaigns using your client knowledge, you need to ensure that you have sufficiently broad marketing consent.

Statements like "I agree to the processing of my personal data for marketing purposes" are likely to be insufficient. When it comes to email marketing, something like "I agree to the processing of my personal data (email address and history of opening messages) for marketing purposes" is much better. In the case of other forms of marketing, **this message needs to be adjusted accordingly**.

Remember that GDPR insists on the clarity, transparency and comprehensibility of messages regarding the processing of personal data.

The user should know specifically what they are agreeing to. You should not use data that you are not sure is covered by consent. Messages that are addressed to the user should be written in a clear, easy to understand way. These messages should not be misleading in any way. Therefore, if you want to use other customer information for marketing purposes than just an email address, you should specify that when obtaining consent from the client.

SENDING MARKETING MATERIALS "FROM PARTNERS" MAY BE DIFFICULT

> *The wording "and from partners" should disappear from the market.*
> *The sale of personal databases may lose their raison d'être.*

If your intention is to send other marketing messages in addition to your own, you should clearly communicate that at the stage of receiving consent from the user.

By "clearly", we mean giving **specific names of entities that will process data in addition to you** or on whose behalf you will send commercial information. The wording "and partners" or "and members of the capital group" is not sufficient.

Sometimes you will be able to limit yourself to indicating a certain group of entities, if it is an indication that is appropriately precise and related to the main subject which the consent concerns. For example, being the head of an association that sends your newsletter, you could write that consent also applies to receiving commercial information "from members of the association".

After GDPR becomes effective, the sale and purchase of databases may be significantly hampered. Even if we assume that people who have subscribed in return for some benefit and have expressed their informed consent to receive marketing content from an unspecified set of senders, GDPR may not recognize that consent as being currently valid.

Also, GDPR will not recognize the validity of so-called “business databases”. This covers databases consisting of public addresses or phone numbers listed on websites, in the records of business activities or in other publicly available sources. For such a case, one has to look similarly to the case of presenting a business card described above. The fact that someone gave me a business card for business contact does not mean that I can add it to my mailing list.

Similarly, **providing an email address on my company website does not mean that you can send me all kinds of business offers**. Of course, this is a contact for people who really want to use my services or otherwise cooperate. By publishing the address on my website, however, I have never consented to receive tourist travel offers, car purchase offers or even business calendars.

THE RIGHT TO BE FORGOTTEN

GDPR introduces the right to be forgotten.
You must be technically prepared to implement such requests.

The rule is that the user may demand that all his data be deleted. There are exceptions, however. Each case of such a request must be considered individually.

GDPR introduces the so-called the right to be forgotten. It means that the data s**ubject may request that you remove all data related to him from your systems and files**. You have to prepare for such situations to know how to technically "forget" someone in your database.

The right to be forgotten will not be absolute. It is about **stopping the processing of data of a specific person** and, above all, **removing publicly available information about such processing** (removing links from the Internet, eg indicating that someone once had an account on a given social network, but deleted it).

The right to be forgotten can not interfere with the security of other personal data. Therefore, **there will be no need to intervene in the back-up**, if it would require excessive technical effort or cost. In addition, preservation of data in the back-up is aimed at a "legally justified interest", meaning IT security. This explains leaving such data in backups, even though all other systems will need to delete the data.

You should remember that the user may request "to be forgotten", particularly if:

- personal data is no longer necessary for the purposes for which they were collected. In particular, when the contract between you and the client has been terminated;
- the user withdrew consent on which the data processing was based;
- the customer did not agree to the processing of his data for marketing purposes;
- the processing involved an electronic service and was based on the consent of an underage person.

The provisions of GDPR regarding the right to be forgotten are a bit more complicated than just the rule "you must always delete all data upon the user's request".
You should remember that this is not an absolute law. Each case of deleting any data should therefore be considered individually (it's possible that there can be a situation justifying the keeping of certain data).

YOU ARE RESPONSIBLE FOR THE SELECTION OF MARKETING SERVICE PROVIDERS AND OTHER CONTRACTORS WHO PROCESS PERSONAL DATA ON YOUR BEHALF

If you use external marketing tools, you will have to choose contractors very carefully.
You are responsible for the selection of subcontractors that guarantee data security and compliance with GDPR.

If you are an entrepreneur, you probably use different types of external tools for marketing, accounting, recruitment agency services, etc. Some of them involve transferring your personal data to your contractor through, for example, uploading a customer database to Facebook or to an email marketing system, placing a recruitment order, having an external accounting office, etc.)

You are mistaken if you believe that the company providing the service is solely responsible for the entire processing of personal data that takes place during this cooperation. Even on the basis of the current regulations, **you are still the data controller and you have many responsibilities as a result.** The subcontractor (the so-called personal data processor) is only responsible for ensuring an adequate level of security for the data provided by you.

Meanwhile, GDPR introduces additional liability on your side. You are responsible to your users, customers, subscribers, employees if you have chosen a provider that does not guarantee the reliable processing of personal data entrusted to it. When deciding to commission a process to an external company - including work on personal data - ensuring their compliance with data protection laws is up to you. In the light of GDPR, you should consider and cooperate only with entities that guarantee the protection of personal data in accordance with the highest standards.

If personal data is processed in your marketing activities, then you cannot choose a marketing tool only on the basis of functionalities or price. You must also **pay attention to the compliance of this tool with GDPR**. Otherwise, you are exposing yourself to legal and financial responsibility.

Joanna Worotyńska
VP of Communication and Marketing @ PushPushGo

Of course, sending web push notifications is not based on the processing of any personal data. However, if you decide to, for example, to collect consent for web push together with an email address, your notification provider will also be the processor of your subscribers' personal data.

Before you use such services, make sure:

- the web push provider **does not use OneSignal, which transparently communicates that they provide their service for free because they resell the data they receive from clients' websites**,
- **its servers are located in the European Union** or in a country where an equally high level of data protection is ensured.

THE PRINCIPLE OF RELIABILITY AND TRANSPARENCY

The most important principles in the GDPR are transparency and reliability.

Treat other people's personal details like money. With this attitude, it will be easier for you to adapt to the requirements of GDPR.

In addition to the principle of data minimization and "privacy by default" that we mentioned above, GDPR also introduces another very important rule, **the principle of transparency and reliability**. The point is that the person whose data is or should be processed has full clarity and the greatest possible control over these processes.

All messages regarding personal data are to be written in clear, easy to understand language. Complicated legal formulas or **phrases written with technical jargon should disappear from the market**.

Requests for personal data can not be misleading in any way. You must not in any way "phish" for personal data or download them "by accident". You must not take advantage of the fact that anyone is unaware that they have shared their personal information. It is also forbidden to base your actions on the ignorance or passivity of the user.

GDPR imposes broad information obligations (explained below). They are not only formal obligations, but real tools that can enable the implementation of the principle of transparency and reliability.

You can assume that the aim of GDPR is to **"civilize" the processes of personal data processing**, which in the present digital world has become very complex and opaque. The metaphor for GDPR's intent that we used earlier still applies: treat other people's personal data like money.

You are **not afraid to entrust your money to the bank**. You probably make online transfers and electronic payments all the time. You're not afraid to pay for an order in an online store in advance. Trading in electronic money is based on trust in all entities involved, as well as on the belief that, in the case of any mistake, any transaction can be settled. If a bank or an online payment operator incorrectly records your transfer, there will be a trace left in the electronic systems and the mistakes can be corrected.

Similarly, GDPR aims to protect personal data. All processes are to be accountable and data controllers must ensure that they do not perform unsolicited operations by users. Simple, right?

EXTENDED INFORMATION OBLIGATION

GDPR introduces much wider obligations than applied before.

Most likely, this means that almost every company operating online will have to have a privacy policy.

Current regulations mandate that if you are a data controller, you must inform the person whose data you are processing about a few basic issues. This includes your identity (the data administrator), the right to request a change in the data or to withdraw consent of data processing.

The GDPR extends these obligations significantly - from a just a few to a dozen or so points. When collecting data from a specific user you will have to provide them with the following information:

- Your identity and contact details - i.e. address details and email address;
- Contact details of the Data Protection Officer - if you have one in your company, just their email address is sufficient;
- The purposes for which you will process the data collected;
- The legal basis of the processing - expressed consent, appropriate law or "legally justified interest";
- Whether you will pass the personal data to some other entity;
- If you intend to transfer personal data outside the European Union - eg to the USA, if you upload them to MailChimp or to Facebook;
- The period during which you intend to store your personal data;
- Information on the right to request access to personal data, rectification, deletion or limitation of processing;
- Information on the right to data transfer - a user may request that his data must be transferred directly from one telecommunications operator to another;
- Information that the user has the right to file a complaint with the relevant authorities;
- The possible consequences of not giving data;
- If you intend to use data for profiling and, if so, what the consequences are for the user.

This information can be made clear in the form of a privacy policy.

WILL THE RULES FOR COOKIES CHANGE? NO. ACTUALLY, YES.

GDPR does not directly regulate the use of cookies. This is dealt with by another piece of legislation, and soon the European Union will most likely introduce new rules on cookies, in the planned **Regulation of e-Privacy**.

However, if you use cookies or tracking tools that allow you to identify the user (not only by name and surname, but also by email or IP address) - then GDPR rules will apply.

Joanna Worotyńska
VP of Communication and Marketing @ PushPushGo

Web push does not use cookies, so you don't have to worry about any changes that the GDPR will introduce in this regard.

GDPR does not introduce changes in the use of cookies, which do not factor in the sphere of privacy of the user.

As a marketer, you have to think about whether you use cookies-based tools in an anonymous way, or whether you are processing personal data.

PROFILING. STILL POSSIBLE, BUT ...

If you are just an "ordinary" marketer, striving to best target your marketing messages, you do not have to worry about GDPR. This type of non-discriminatory profiling will not be banned.

You must, however, consider whether or not you will violate the rules of GDPR if you use "automatic decision-making" on serious issues that can significantly affect the situation of your clients, leads or users.

It is not true that GDPR prohibits profiling and that it will only be possible with the express consent of the user. Profiling as is used in most marketing processes - displaying personalized ads or marketing messages - **will be allowed without the user's consent,** within the framework of the so-called legally justified purpose, which is the marketing of your own services and products. You will not have to collect separate consents. Nevertheless, it will be necessary to **inform users that you are profilling them**.

On the other hand, profiling will be banned (unless the user agrees) if it "automatically makes decisions that **produce legal effects** or other similar effects". It's a bit of an enigmatic statement and it is difficult to say in advance what these "other similar effects" are. However, it is about serious issues that affect the sphere of privacy of users or their personal and economic situation.

Certain profiling of clients that leads to discrimination will be forbidden. For example, a real estate office cannot make automatic decisions about who can live in a given neighborhood. Displaying offers of the same product to different people at different prices will also be prohibited. You must obtain user consent for such activities and provide them with the right to object to profiling.

However, an automatic process that determines whether a given store may display, say, an advertisement for a blue or green T-shirt is not one of these "serious decisions". You can still use such profiling after GDPR becomes effective.

YOU MUST HAVE DOCUMENTATION FOR EVERYTHING AND BE SURE THAT YOU ACT IN ACCORDANCE WITH THE LAW

GDPR puts a lot of emphasis on the principle of accountability, the ability to check at any time which aspects of personal data processing are used in your company.

There is virtually no way to ensure this accountability in a different way than by introducing different types of policies and instructions and making sure that they are applied on a regular basis by all employees in the organization.

We've already mentioned the principle of transparency and accountability. It is also known that on the basis of GDPR, companies will be **subject to fines from the relevant authorities**. It is your company's role as data administrator to bear the burden of proving that you have taken all actions in accordance with the new rules regarding the protection of personal data.

It is unlikely that you will satisfy the requirements of GDPR unless you take specific steps to reorganize and restructure the way you handle personal data in you company and all relevant policies regarding the storage and processing of the data.

If you do not have a **formal, organized plan** for conforming to the regulations imposed by GDPR, it will create many opportunities for you to commit violations of the many demands that it makes. Conforming with GDPR requires a careful and deliberate plan of action.

GDPR also introduces **an obligation to maintain a "personal data processing register"**. It will be mandatory for virtually any company that processes personal data to any significant degree.
It seems, therefore, that these procedures will apply to every company.

USING AMERICAN TOOLS? CHECK YOUR CONTRACTOR

GDPR does not prohibit the transfer of personal data to the US contractors.

In order to use American tools for marketing purposes, however, you need to check whether your contractor meets the security standards as they apply in the EU.

In the maze of online information about GDPR, you may have heard somewhere that it will be **prohibited to use any American tools**, even with the consent of the user. **It's not true.**

GDPR does not intend to block the exchange of data between EU and US companies, but it clearly indicates that it is necessary to **carefully select potential US counterparts**. It is your company who is responsible for whether the US contractor actually provides adequate data protection.

According to GDPR, it is always better to choose EU contractors to **ensure a greater likelihood that they have also adapted to GDPR regulations**.

As an EU entity, however, you will be able to send personal data to US counterparts (and use US applications) if at least one of the following conditions is met:

- the American entity is inscribed on the so-called Privacy Shield list,
- the transfer of data to the US is necessary for the performance of the contract between you and the data subject (if, for example, you provide courier services to America, it is obvious that for the execution of orders would be necessary to transfer personal data to the US - because you need to transfer recipients in the US. information about the sender from the EU),
- the person whose data is processed has to be informed of the potential risk and expressly consent to the transfer of his data. It does not have to be written consent, it is just important that it is clear,
- you will sign an extended agreement, set by the European Commission, in line with the so-called standard contractual clauses with an American contractor.

At present, American companies pay much more attention to the protection of personal data than just a short time ago. Most of the significant entities are certified and entered into the Privacy Shield list. Others offer signing agreements in line with EU guidelines.

THIS IS SERIOUS BUSINESS WITH MORE THAN FINANCIAL PENALTIES

> *Violations of GDPR can result in more than financial penalties.*
>
> *In case of an inspection, authorities will be able to temporarily order you to stop specific activities related to the processing of personal data.*

You may have heard that **GDPR is a very restrictive and burdensome legal act for marketers** because it introduces new requirements and significant penalties for violations.

The truth is that GDPR presents **challenges for companies operating online**. Authorities will be able to issue a so-called provisional order. Such a decision allows the authority to be able to order the cessation of certain activities related to the processing of personal data.

For some entities, this may mean closing their business altogether or **closing their marketing activities for a longer period** - until the matter is clarified..

GDPR is a serious business issue but manageable with the right knowledge and approach.

CONTACT US

Joanna Worotyńska

VP of Communication and Marketing @ PushPushGo

joanna@pushpushgo.com

Agnieszka Grzesiek - Kasperczyk

Legal Advisor, Partner in MyLo law office

agnieszka.grzesiek@mylo.pl