THE **GDPR HANDBOOK** FOR CONCERNED MARKETING TEAMS

TABLE OF CONTENTS

If you are not worrying about it by now, you should.

The General Data Protection Regulation (GDPR) is upon us and with it the need for an everlasting data management system.

Ultimately, we all know that this complex set of rules means to protect both users and marketing teams and that is a good – and very necessary – measure.

On the other hand, it also means a huge hassle to demonstrate what should be obvious by now: we are all making our best efforts to keep people's data safe and oversharing their information never was, nor will be, an option.

We're going to kick off this handbook to the GDPR with a 101 on the most relevant traits of the legislation. No matter how big or small your company is or how many data sources you use to enhance your marketing strategy, these guidelines will definitely come in handy.

After that, we will get into some more specifics traits of the legislation, aiming at **understanding exactly what a Marketing Team can expect for its data management endeavours.**

We hope you will find it helpful and at least a little bit entertaining.

GDP-*what*?

The General Data Protection Regulation (GDPR) is a set of rules that intends to:

1. Avoid the abusive collection and use of personal data

2. Restrain and supervise the way companies share that data with others

The GDPR defines when data processing is lawful, and its scope tries to balance between users' rights and the companies' pursuit of legitimate interests.

THE SCOPE (art. 3)

First things first: **who does this affect? Almost everyone**, actually.

If you run a business within the EU, you have to observe the regulation and if you are not in the EU but in any way collect or store information about EU citizens, you also have to observe the regulation. Even worse, if you're not an EU company, you might have to name a person there to represent your interests.

FINES (art. 83)

Breach of legislation comes with a very, very heavy price.

Fines range from €10M OR 2% OF THE COMPANY'S REVENUE **to** €20M OR 4% OF THE COMPANY'S REVENUE**, whichever is higher.**

The second tier of fines refers to the most blatant infractions, namely those that have to do with data transfers and basic principles for processing, such as the absence of consent.

The first one refers to "minor" infringements: privacy by design and by default infringements, lack of activity logs and so on.

INTO THE SPECIFICS

This next chapter focuses on some of the most intricate lines of the GDPR: **Privacy by Design, Pseudonymization, and Data Deletion.**

They may sound like a complicated bunch but we tried to skip Law terms and use examples as much as possible so this wouldn't get dull and cryptic.

So let's take a deep dive into the GDPR. It's going to be fine. We're right by your side.

PRIVACY BY DESIGN (art. 25)

Privacy by design simply means that **as soon as you start outlining your data collection activities** you should bear in mind the safety of the data you are collecting, and take the careful and logical steps to make it inaccessible to people who shouldn't access it in the first place.

You must be able to demonstrate your compliance to users and the authorities, and this means you will have to **document all of your data data processing endeavours**.

In case you already collect data, you will have to rethink and document your process with data privacy in mind.

PRIVACY BY DEFAULT (art. 25)

This can be subsumed under the premise "what you sign for is what you get".

We've all been there: to sign up for a social media service, the required fields name and e-mail. You end up filling up the fields age and city of residence because you're used to it. Once your profile is fully set up, the fields age and city of residence also show up publicly. Under the GDPR that is a breach of regulation, because all that they needed from you was your name and e-mail.

Data minimization, the notion that you should not collect more data than the one you really need, plays an important role here.

Companies should begin data management procedures with this question: **"What's the absolute least information my company needs from a user?"** And then they need to stick to their answer.

PSEUDONYMIZATION (arts. 4(5), 25 & 32(1))

The GDPR legislation specifically focuses on Personally Identifiable Information (PII) and the logic is quite simple:

If you can identify a person, you cannot use their data.

How do you identify a person according to the GDPR?


NAME


ID NUMBER


GEOLOCATION DATA


COOKIES

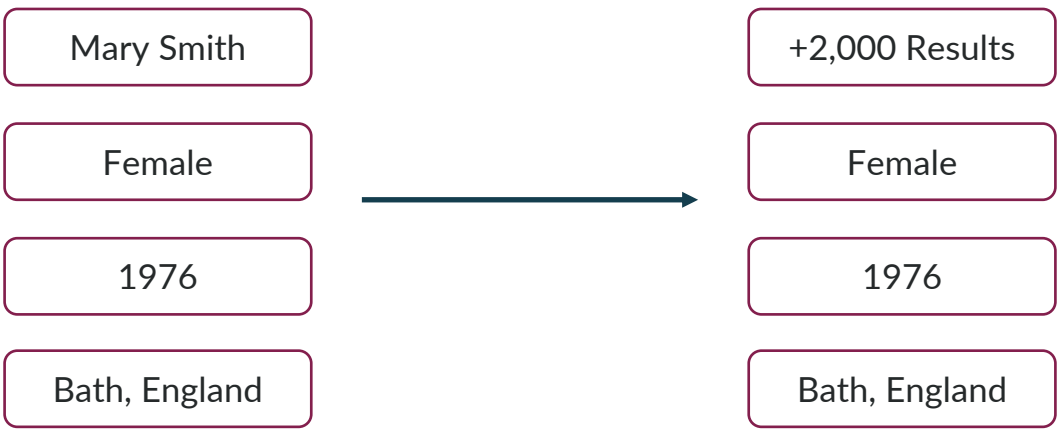
And many other biosocial components.

However, the Regulation clearly states that **you can use Pseudonymized data**.

When you pseudonymize data, you separate PII from non-PII, keep them in separate data silos and make sure to throw away that key.

On top of that separation , it is still are highly recommended that you encrypt the additional information.

For instance, imagine you have a database with the fields “name”, “gender”, “year of birth” and “city of residence”.



If you take away the field “name” and put it in another database, the remaining fields by themselves cannot identify a person (how many females born in 1976 live in Bath?).

DATA DELETION (art. 17)

To shed some light into another matter that was quite blurry and raised many questions, the GDPR consecrates users the right to data deletion. This is also known as the right to be forgotten or, as the Regulation itself calls it, the right to erasure.

This right is not absolute, but it does apply in these situations:

- **Unlawful processing (breach of the GDPR)**
- **Requested by the law**
- When the data is no longer necessary for the purpose it was initially collected for
- If the individual explicitly withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

The right to data deletion is something to bear in mind from the beginning of your data management strategy, not only because it rebalances a user right that was missing, but also because it is one deeply associated with brand trust issues.

USER CONSENT (art. 7)

Even if the absolute need for user consent is still under discussion (we'll look into that in the next chapter), companies should still know what the guidelines are so that they can set themselves up for GDPR compliance.

ISOLATED: not amid the terms and conditions

IDENTIFIED: not only your organization but also 3rd-parties you rely on.

ACTIVE: no pre-ticked boxes

EASE OF WITHDRAWAL: tell people how (and where) to withdraw consent straightaway)

DETAILED: different types of processing means different boxes to tick

INTO MUDDY WATERS

The muddy waters of article 6(1)(f) and the to-be-approved ePrivacy Regulation are so specific we relied on the expert help of Dr. Christoph Bauer, CEO of ePrivacy, for this specific part of the handbook.

OPT-IN, COOKIES, AND ARTICLE 6(1)F: A STATE OF THE ART

Let's jump to the crux of the matter, the GDPR article listing criteria must be met to lawfully process data:

> *1. Processing shall be lawful only if and to the extent that* ***at least one of the following applies:***
> *a)* ***the data subject has given consent to the processing of his or her personal data for one or more specific purposes****; (...)*
> *f)* ***processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party****, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

This particular moment of the GDPR brings two alternatives to the table: for marketing purposes, you either create an opt-in to be able to collect data or your marketing initiatives clearly fulfill the legitimate interests clause.

How far can the legitimate interests of a company take you?

Prof. Dr. Christoph Bauer is the CEO of ePrivacy. ePrivacy advises and supports companies in the digital economy with all aspects and challenges of data protection. They are based in Hamburg, Germany, where data protection laws have been famously stricter than almost anywhere else. They think of data protection as a competitive advantage, and their independent consulting and certification offers have helped the likes of Criteo, Acxiom, Krux, and Huawei.

THE LEGITIMATE INTERESTS' PATH

This is exactly the type of question ePrivacy's experts can answer swiftly. When we reached out to Prof. Dr. Bauer with this question, his clear answer was rather reassuring:

> *This clause* ***grants legal permission, not only for classical direct marketing methods, but may also be applicable for online behavioral marketing measures, given that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest"*** *(Recital 47 of the final Regulation). As a consequence, it will be possible to use personal data with the interest of direct marketing, as long as the interests of the data subject concerned are not overriding the marketing interests. (…)*

Furthermore, he believes that this particular stance of Recital 47

> *The legitimate interests of a controller, including of a controller to which the data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on the relationship with the controller.*

shows a "notable shift towards the US approach to data protection, given that the 'reasonable expectations of users' are evidently set to become the central point of departure for any consideration of this issue in the future: data, which users can reasonably expect to be processed, can be processed without the user's consent – even by a third party".

THE REASONABLE EXPECTATION'S INTRICACY

Despite the optimistic feeling to all of this, Prof. Dr. Bauer does have a **few caveats**:

> *In the future, most business models in the online industry will not require data subjects to give their consent to the use of their data, provided they stay within the bounds of their users' 'reasonable expectations'.* ***The true scope of the 'reasonable expectations' criterion remains to be seen.***

He does, however, have a few suggestions to make on this regard:

> *It may well make sense for companies to refer to such 'reasonable expectations' in their individual data protection declarations or privacy statements and, thereby, to include them into the scope of this criterion. (…) As the legitimate interest is quite new, it is even more difficult to draw a line, so probably both parties – authorities and the industry – will be quite careful to conduct an aggressive approach.*

THE PROPOSAL FOR AN EPRIVACY REGULATION

A game-changing regulation that focuses on the wellbeing of European Union's online advertising landscape. Its intricacies are such that we resorted to ePrivacy's CEO, Prof. Dr. Christoph Bauer, once again for some expert insights.

THE ROAD SO FAR

The recent nature of online data collection brought with it a severe lack of regulation. That absence of control lays at the core of the EU's decision to implement the GDPR.

The complexity of the subject is such that the European Commission built yet another set of rules regarding online data collection and processing: the Proposal for an ePrivacy Regulation. This proposition is missing approval but its enforcement is due to begin on May 25th 2018, just like the GDPR. It aims at replacing the ePrivacy Directive 2002/58/EC, which is fairly outdated.

But this Proposal for an ePrivacy Regulation raises new problems, the emergence of the matter being the smallest of them.

WHAT'S THE DEAL WITH THE EPRIVACY REGULATION?

The Proposal for an ePrivacy Regulation clearly stands by the need for consent the GDPR already foresaw.

Where it deepens the GDPR assumptions is on its understanding of where to define the **frontier for third-party cookie collection**. While information on cookie issues is to be found on articles 8 and 9, recitals 21 to 24 focus on the tracking and third-party cookie issues. The proposed document goes as far as stating **the decision on which cookies a company can collect should be set by the user at browser-level.**

This means you decide whether or not a company can collect data about you even before you open their website, and while that ensures the end-user won't be hassled by some companies, it also means they won't be reached by those they might like to hear from. And this is only the beginning of the problem: if we move the needle from end-users to companies' perspective, the problem is much more complex.

WHAT DO EXPERTS THINK OF THAT?

We leave it to Prof. Dr. Christoph Bauer, from ePrivacy, to draw conclusions from these assumptions:

> *"This regulation would dramatically change the Internet like it works and is used now. Many publishers offer their content without separate remuneration, but in return ask the user for certain data, e.g. to optimize the distribution of advertising which finances the content. As it is not probable that users directly opt in for cookies, many publishers won't be able to maintain their offerings. The same applies to technology providers that work with these data and an opt-out mechanism. For them as a third party it will hardly be possible to achieve the opt-in of the users. These providers will need to change their business model significantly and there is a danger that they will have to stop their businesses completely."*

This position is fairly widespread throughout the online advertising landscape, but there is much debate and consensus is not within sight. Nonetheless, **IAB Europe's CEO Townsend Feehan agrees that the current draft would render online advertising nearly impossible.**

Ongoing between the EU representatives of advertising and people's groups are trying to find a common ground on the topic. The last meeting took place in the days of September 2017, so more information on this subject is expected to arrive anytime.

THE **GDPR COMPLIANCE** CHECKLIST

It's easy to get lost with all the information around the GDPR. So, because there is much to learn and many changes to adapt to, we prepared a checklist with the basics on the changes your company will need to undergo on the path toward compliance.

ASSESS YOUR DATA

- [ ] Know and distinguish the types of data you collect (PII and non-PII).
- [ ] Define consent types, one for each data collection purpose. Make sure they are clear, unambiguous, and detailed.
- [ ] Assure the users' right to withdraw consent and clarify that it won't affect the way you deliver your content to them.
- [ ] Define a clear timeline of how long you intend to keep the data and ensure you keep it up-to-date.
- [ ] Raise the safety bar: consider pseudonymization and encryption procedures to protect the personal data you hold.
- [ ] Invite-only club: make a list identifying the people who are authorized to access the data.
- [ ] Beware of the special categories: children's data, biometric or genetic data et al. have to meet specific standards of security (art. 9). Have them at the tip of your tongue.
- [ ] Analyze whether or not your company requires a Data Privacy Officer and/or a Data Privacy Impact Assessment.
- [ ] Where is the data: Data that is transferred from the EU should have specific protections (chapter 5) in place. Make them happen.

CHANGE PROCEDURES

- [ ] Define procedures to systematically implement safety by design and default rules in every new project or initiative.
- [ ] Get the whole team onboard: have everybody know the basics of the legislation.
- [ ] Find solutions for how to deal with users' requests for data access, update, and deletion.
- [ ] Define procedures for swift action in case of data breach.
- [ ] Review and audit data **and** procedures regularly.

SET UP DOCUMENTATION

- [ ] Create an internal document that subsumes every participant in the data processing endeavors, their roles, responsibilities, and reporting lines.
- [ ] Have a general, easily accessible document with contacts and procedures in case of security breach.
- [ ] Keep an updated and detailed record of data processing activities that includes purposes of processing, data categories being processed, security measures, and a data flow map.
- [ ] Update contracts with third-parties reflecting your new data strategy procedures.

IN CONCLUSION

"First of all, I cannot stress enough how important and needed this legislation is. Being on the business for many years, one truly gets to see how much companies have softened their perspectives on data awareness. For me, it's not just the quick buck, I like to believe this is the natural way of dealing with new opportunities: eventually you get so tangled up in the way things are done, you just end up assuming it's the right way to do it.

This is why I believe that, even if the General Data Protection Regulation and especially the ePrivacy Regulation are flawed, they are still better than what we had.

Velocidi has long been an advocate of an alternative way to do data management and I can't help finding it reassuring that premises like Privacy by Design and Default or Pseudonymization have come to our mind long before the legislation was approved.

This being said, I think that the key takeaway here is: change and adapt. Rethink your procedures from scratch. Get specialized help if you need it. But don't make the mistake of letting the GDPR slip from the top of your to-do list. The clock is ticking."

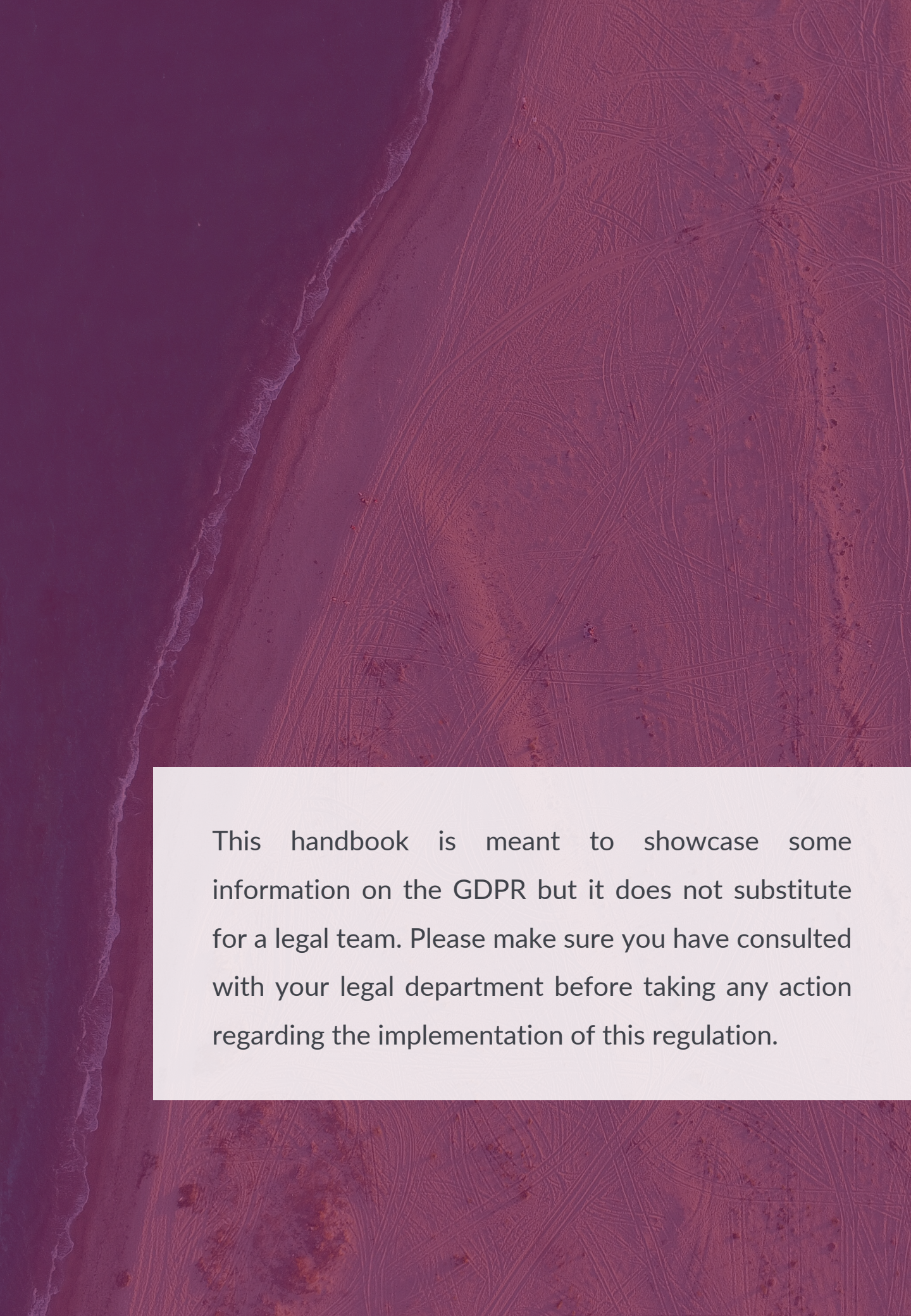
Velocidi Chief Product Officer

Paulo Cunha

We would like to thank the people at **ePrivacy** for their contributions and guidance on the most complex subjects. Look them up if you need expert advisory on these matters: they are the absolute best.

And we could not let you go without telling you about the **Velocidi CDP:** it will come in handy.

With it you can combine both media and customer data in one integrated system to create the most thorough and accurate customer profiles. Plus, its user-friendly analytics and reporting tools let you easily uncover opportunities to drive down customer acquisition costs, increase conversions, and optimize margins. All of this comes with the benefit of single tenancy, in a private cloud or on-premise deployment, where Velocidi clients are the sole controllers of their customer data.



This handbook is meant to showcase some information on the GDPR but it does not substitute for a legal team. Please make sure you have consulted with your legal department before taking any action regarding the implementation of this regulation.

velocidi

Visit us at www.velocidi.com to learn more.