GDPR for Financial Services Marketing

How to translate data regulation into customer opportunity

Contents

1. Turning fear into opportunity

The financial services sector is under tremendous regulatory stress, driving traditional banks to adapt to new and more agile approaches. Customers, meanwhile, are empowering themselves to manage money in a way that works for them. Convenience has become the new loyalty.

Marketing has no easy part to play in this new world: how do you communicate with individuals when they have a world of money-managing tools at their fingertips, and where knowledge is freely shared and prices are easily compared?

As a marketer, you are constantly trying to achieve and maintain that competitive edge, by, for example, unlocking new market segments through second and third party data providers, or by retargeting your existing customers. This data from a variety of sources is shared across teams, and across platforms.

But how confident are you that you are not opening yourself up to inconsistencies - even vulnerabilities? How sure are you that the data will not go on to lead a life of its own, which might open your company up to liabilities and litigation? How should you approach your customers' flexible adoption of services, while balancing this with their corresponding privacy concerns?

Furthermore, how should you incorporate new data privacy regulations, while giving your global and regional teams the tools they need to engage in ever-more personalized and contextual messaging - across the network of online and offline channels you already have in place? How do you translate your customers' concerns about data privacy?

This paper looks specifically at the implications of the EU's upcoming General Data Protection Regulation for marketers, and how you can leverage this change to achieve a 'win-win' situation, by re-establishing a lasting demand/supply relationship, built on trust and openness.

2. GDPR will reshape modern marketing

So, what is GDPR?

GDPR is the European Union's General Data Protection Regulation, which will take effect on May 25th 2018. It is the biggest overhaul in security and privacy regulation since 1995[1] – the 'cellular' epoch and a time before widespread use of interconnected internet channels and smartphones.

The world as a connected entity is changing at breakneck speed. In this ever-evolving digital and physical world, we can assume that the governing regulations will receive a facelift too. This is exactly what has culminated in the GDPR updates. Key to the changes is giving the power of ownership back to the individuals whose data is being captured and processed.

This new regulation has many facets but most importantly it nudges companies towards a "privacy by design-approach," forcing companies to put privacy and security considerations to the top of their priorities.

> *Companies need to rethink their organization, becoming more customer-centric and putting the customer's journey and their experiences on that journey at the center of their operations. The empowered customer can switch banks at any moment – so how do you engage with such a customer? By being relevant, credible, and reliable.*
>
> ***Julius Abensur***
> *Financial Services Director*
> *Relay42*

More importantly, this shifts privacy and security from an IT challenge, to a company-wide challenge.

GDPR applies to any company working with EU citizen data - which is referred to as personal data, which is personal identifiable information – including customer and employee data. Since virtually all companies have some Customer Relationship Management (CRM) systems or record of customer interactions, this regulation will affect virtually everybody.

In addition, GDPR places pressure on companies to actively manage, live, breathe and prove compliance. Effectively, this means that companies need to show that they are compliant and what measures they've employed to be so. The regulation is 'incentivized' by significant fines for non-compliance. These can reach up to £20 million or 4 percent of global revenue, whichever is highest.

These topics have all been extensively covered in several whitepapers and documents, describing basic compliance preparations[2, 3] and the most important areas covered by the GDPR[4]. All these documents provide valuable knowledge on the subject but remain on the surface in terms of technical solutions or specific areas of focus. Therefore, this report focuses specifically on the implications for marketers and the marketing function. In particular it looks at how to open up new market segments while taking an agile approach to GDPR compliance in the marketing space.

To understand the perspective of marketers confronted by GDPR, we surveyed a group of practice experts holding various marketing and digital roles at the CxO level at major corporations in the United Kingdom within the Financial Services Industry. Their expert positions across these various companies make their responses especially valuable and form the statistical basis for this report.

What are the implications for marketers?

The marketing space is one in which the regulation's influence is especially prevalent. This field is defined by the personal identifiable information it collects and uses. For every interaction that is personalized, contextualized or relevant to a customer's behavior, information on that specific person is captured, stored and used in the process.

Each of these data points constitutes personal data and is subject to the regulation. Without the customer ever knowing, modern systems seamlessly capture millions of personal identifiable data points per day.

GDPR regulation states clearly that the capturing, processing and use of this data needs to be limited to the specific purpose it serves and is subject to authorized, informed consent. It should also be timely information and replaced or updated when new information surfaces. If anything, the regulation is a pushback on the Big Data zeitgeist that sometimes appears to see no limit in data accumulation.

This means for a company that all areas that handle, store, or process data should have a clear understanding and grasp of the regulation's scope – as well as the scope and purpose of the data. But this is especially true in marketing, where personal data forms the very structure of their reality, and so the regulation should be well understood and enforced.

How many integrations (channels, databases and systems) do you have in your digital marketing space?

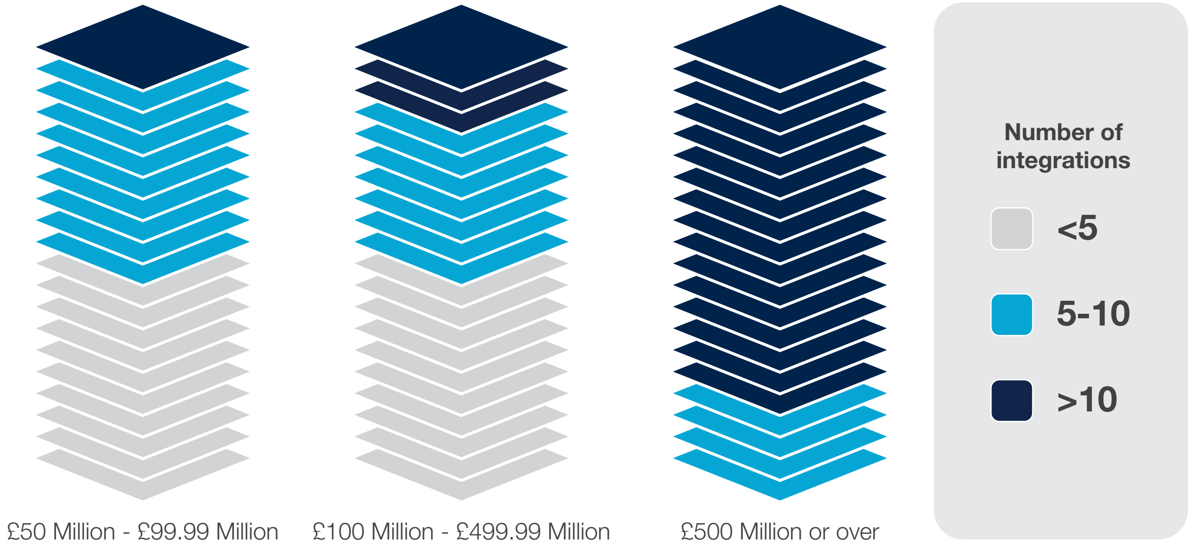

Figure 1
Source: Censuswide Research, May 2017

This is a daunting task, especially when you consider that more than three-quarters of the respondents in our survey who work in large organizations (with an annual turnover of over £500 million) say that their companies employ 10 or more integrations (customer channels, databases and systems), see Figure 1.

Additionally, our respondents indicate that they work with multiple agencies who, in turn, also work with a variety of integrations - adding to the complexity of the digital landscape. Each of these integrations is usually handled by its own department, usually without clear oversight or governance.

An integration is a second or third party instance you collaborate or work with in order to reach your marketing goals. Google DoubleClick, Facebook Custom Audiences, and Clang are some widely used integrations. The complete marketing landscape consists of nearly 3,500 such integrations[5] all of which are commonly fed by customer-specific and personal data.

Our respondents also confirm that this data is invariably classified as "personal identifiable information", and four-fifths of the respondents indicate they don't always know who has access rights to the various data sources (see Figure 2). Only one fifth of respondents are fully confident of being able to identify who has access to the various sources of data.

Although almost all of the respondents claim they have a central overview of the customer data, they don't know whether customers have opted-in for the gathering of this specific data.

Do you know who has access rights to each marketing application?

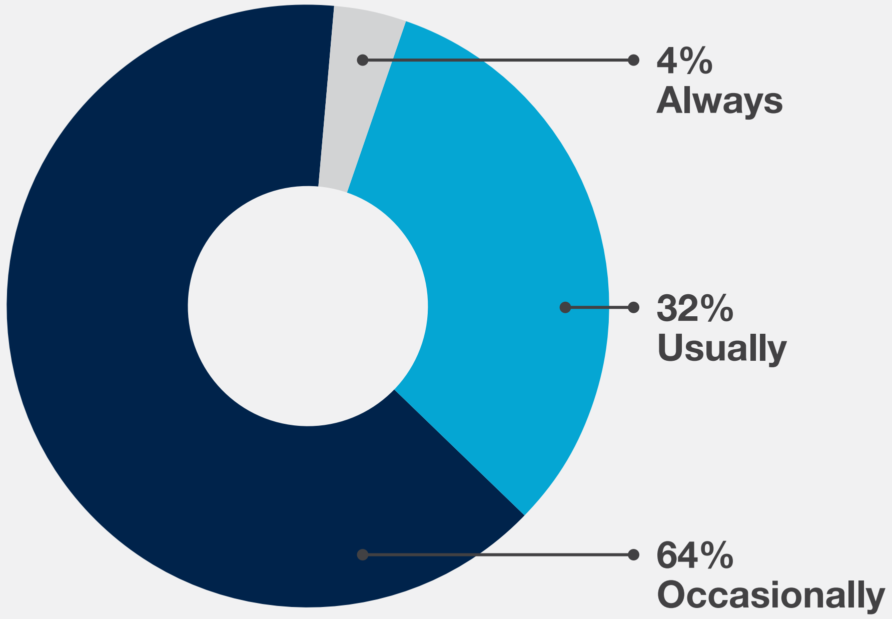

Figure 2
Source: Censuswide Research, May 2017

3. Managing the data protection paradox

How to unlock segments, create new audiences, maintain omni-channel relevance… and stay within the regulation

While these changes for the Marketing function could be viewed with a sense of dread, we believe, on the contrary, it is, and should be, considered an opportunity- to take command of the situation. Firstly, to prepare and organize now, before the data that generates your biggest business value becomes your greatest liability.

The transparency and relevancy — or lack thereof — delivered because of these changes could probably change the perception of your brand. It could alienate your customers, or make them stick around for longer. It could drive them to competitors who have exercised greater care and precision, or it could create lasting relationships because you value and protect their data. It could result in fear, or be embraced as an opportunity. This is the essential paradox.

4. Resolving the core data protection challenges

So how to address this paradox given the challenges of the hyper-connected customer, set alongside the limits set by the new regulation? In answer, we focus on three key areas. **Data locality** (where is the data?), **data security** (how safe is the data?), and finally **data access** (who can access the data?). These dimensions will be used to highlight the impact of the regulation on the marketing landscape, and to explain or define the solution space. In short, what can Marketing do to turn this change into the building blocks for commercial success?

The solution

Ideally, your company employs a central orchestration tool for your marketing activities that offers the freedom of relaying data to all the integrations you use in daily routines, a technology which shouldn't be obstructive to your business objectives and infrastructure.

Data locality: a scattered landscape of channels and data

As previously highlighted, a problem that is specifically ubiquitous in the marketing practice is the multitude of integrations - channels and platforms that are employed in daily operations. Each integration requires a specific upload document containing different pieces of personal data. This is to find your customer and engage with them in the most relevant way, wherever it would seem most fitting: social, on-site, or via third-party domains.

The regulation indicates that not only the structured data (in the non-technical use of the term), but also importantly the unstructured data is subject to a breaches and leaks notification. Structured data, here, refers to data organized in a clear and defined system, such as a database, platform, or customer relationship management system. Unstructured refers to data that does not reside in databases but rather in emails, content sharing sites, social media, videos, photos and personal devices.

Banks are not unfamiliar with breaches – in fact a recent Capgemini study reported that one in four banks have been victims of a hack[6]. Once information is uploaded in these systems, it should be easily deleted or changed - leading to differences from the original file. The source, however, is usually unavailable to these integrations or systems. The data imported into the systems and exported from the source is usually sent through email, or by another means of data-sharing.

Our survey indicates that more than half of the CMOs and CDOs had received some form of personal identifiable information in their mailboxes or other unmonitored device in the last year (see Figure 3). These data-exports are exceptionally hard to find or trace, due to their decentralized and siloed nature.

Have you received a data export in your mailbox or other unmonitored device in the last year (e.g. usb, email, dropbox, etc.)?

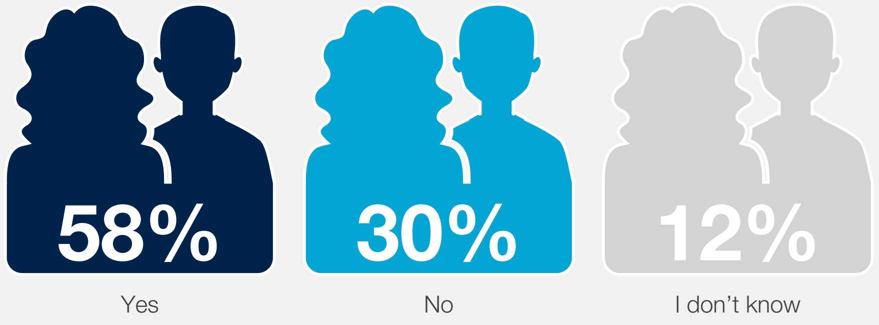

Figure 3

Source: Censuswide Research, May 2017

Data security: technical solutions for complex data security

GDPR has very clear boundaries for the most part. It concerns data that is personally identifiable, and data relating to citizens of the EU and EEA. This means that, for instance, cartographic geographic information is not subject to the regulation, and also, when a cluster of data is made anonymous (stripped of all direct references to a personal identifiable piece of information), it is no longer subject to the regulation.

There are three “security levels” that you should be able to activate to various degrees, meaning you can manage regulation changes with a greater degree of control. Although any of the following should be considered as part of a spectrum of activities, we consider a trichotomy of levels:

The solution

As a marketer, you should be able to set these levels of security without having to understand the underlying mechanics or technical implementation.

Anonymization

This level changes, for instance, a subject (customer’s) name into a category. This is called data aggregation and means that from the pool of data it is impossible tto re-identify a single subject. This means that ages can be stored as age-categories, or that names can be substituted with gender identifiers.

Anonymization effectively forgoes your obligation to be GDPR compliant since it is no longer considered personal data. It is important to take note of the fact that rules for making data anonymous are especially stringent. It means that neither you nor *anybody* else can reproduce a dataset containing personal data, — even if the second party holds additional information.

Ways of anonymizing include noise addition, substitution, aggregation, and differential privacy.

Pseudonymization

Pseudonymization is a way of making the information not directly recognizable. It requires considerable effort to decipher the data gained in a breach.

Pseudonymization introduces some leeway in the breach notifications. It means you have longer to identify what was leaked or stolen in a breach and gives some additional time for reporting breaches towards authorities and affected subjects.

Possible solutions for pseudonymization include hashing[i], and salting[ii].

Encryption

Encryption is processing data into code. It renders the code useless to anyone who doesn’t have the key to unlock the code.

Like pseudonymization, it gives some breathing room in the notification of the authorities in case of a breach. It is not a carte blanche to forego other security measures.

Encryption solutions include symmetric and asymmetric variants depending on the goal, with varying bit-lengths for increasing security measures.

The solution

Centralizing your marketing operations and security orchestration gives you a significant advantage. It helps you to organize role-based permissions in a single location, and allows you to set up processes to add, change, or revoke user access rights by the business itself. The proper control of data access rights ensures your credibility as a company and as a brand.

A relatively simple framework is a practical way to begin structuring and managing permission levels and roles, across multiple platforms (see Recommendations).

Data access: role-based permissions for your entire digital landscape

These data sources, scattered or centralized, have different levels of permissions and access requirements. Some pieces of information might be free for all to see, while some might be very sensitive and for a specific group only – or for nobody. These levels of permissions are called “data access rights”. Despite this, some are still left wondering, who has access to which piece of information?

Our survey of CxOs in the FS sector in the UK showed that more than half of the companies do not have a clear overview on who had access to different systems (Figure 4).

The respondents also claim that in the majority of cases, permission levels were set by IT, and only a small fraction by marketing departments themselves (Figure 5).

Permission levels are generally set based on a user’s broader department needs and not, for instance, tailored to the specific requirements of the user’s role. This can be problematic because of the complex nature of user roles within different company practices, such as marketing. It makes for a compelling argument that on top of all other security measures, it is crucial to take note of who has access to data.

The Currency of Trust paper by Capgemini showed that “74% of consumers would switch bank or insurer in case of a data breach”[6], so taking the right approach to permission levels is paramount in retaining your customer base.

Is there a clear list of people who have access to different systems and applications according to their roles inside the company?

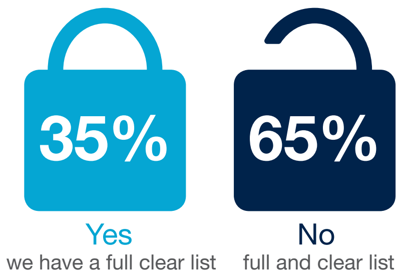

Figure 4

Source: Censuswide Research, May 2017

Who is responsible for granting access permissions to different systems and applications in your organization?

24%	78%	2%	42%
HR	IT is responsible for access permissions	Marketing can set their own permissions	Direct Manager

Figure 5

Source: Censuswide Research, May 2017

*Respondents provided more than one answer

5. Unleashing the full potential of your information

A Data Management Platform as the command center of your marketing integrations

In the marketing field, a solution that centralizes the increasingly complex network of integrations, platform experts and regulations is a Data Management Platform (DMP). From a marketing perspective, this is a unifying technology that not only organizes, but orchestrates messages across any and all customer channels and touch points, both current and future. In this way, marketers can deliver seamless journeys at scale, reflecting individual customer preferences and behaviors.

In addition, a DMP is a command center for your integrations network. It is a central place for security orchestration, creating a clear space where data can reside, eliminating the redundant data clusters and data-exports. It allows you to set specific privacy and security measures, as well as clear user permissions, based on company role.

But what really sets DMPs apart from other solutions? In short, the right DMP allows you to take control. Rather than employing post-fact pattern recognition software to detect breaches for example, you can avoid these problems and instead create a robust marketing environment that aims to eliminate these breaches altogether.

Many companies struggle with legacy systems and complex architectural landscapes. There is a compelling case to be made to assess all potential flaws or liabilities to breaches. But this assumes a passive and reactive approach and is about patching the existing landscape. However a DMP can adopt a more proactive stance towards security and privacy orchestration. It's about bringing value and security to your company; not one or the other.

This new agile approach to privacy comes with the territory if you work for a young start-up; companies that don't consider privacy and security as an afterthought, but as an integral part of their existence and built in from the start. It is what has made them challenge if not beat the traditional competitors in the first place. So for companies with large legacy systems, a DMP creates a unique opportunity to begin changing its traditional approach from reactive to proactive.

Meeting company-wide GDPR regulation starts now

Although this report is aimed at the marketing practice, marketing is not the only functional domain to be impacted by the new data protection regulations. GDPR is all encompassing. It is already finding its way into every part of your business. Our respondents indicate that they see GDPR compliancy as being almost solely an IT and Legal responsibility (see Figure 6, where more than one answer was possible).

> *"GDPR offers companies a unique chance to rework their customer strategy, changing a reactive stance into a proactive one. It provides an opportunity to re-engage in a more productive dialogue with their customers, based on real transparency and openness, secure personal data, free choice and personalization. This is a stance that needs to be enabled by technology – using a nuanced, robust data management platform."*
>
> ***Ron Tolido***
> *Global CTO Insights & Data*

Who is responsible for being GDPR compliant in your organization?

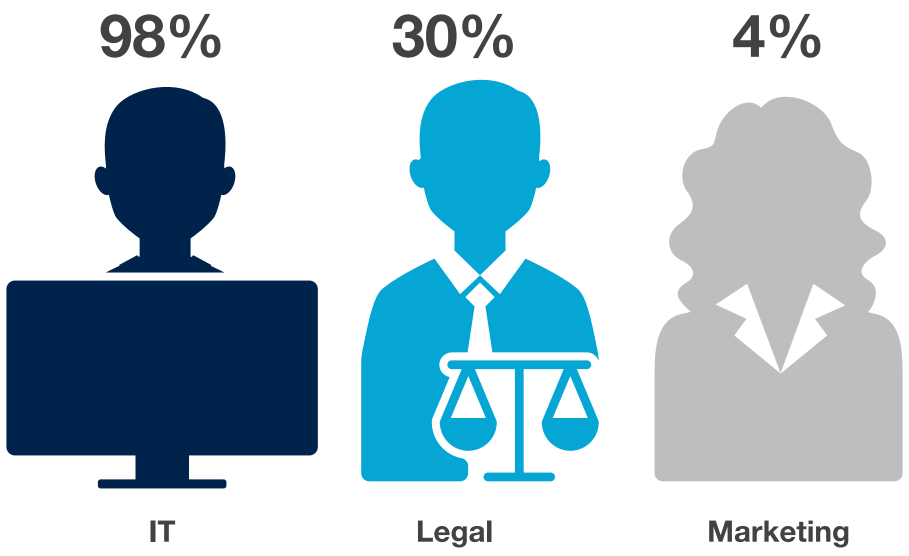

Figure 6
Source: Censuswide Research, May 2017

Only a very small percentage consider that this responsibility is shared with marketing. The truth is, GDPR compliance has to be shared across all functions in an organization. This means every — yes, every — practice or department in the company needs to be aware of, and proactively preparing for, the upcoming changes.

The Capgemini *Currency of Trust* survey[6] summarizes this nicely: "They [companies] need to reinforce their cybersecurity defense program with state-of-the art security intelligence and breach detection capabilities. This, however, must be coupled with the right data practices if security investments are to deliver upon their potential. With this integrated approach, banks and insurers can continue to earn their customers' trust and build a winning skillset in a world where the amount of data that flows between them will only increase".

6. Recommendations

Contrary to much of the GDPR hype circulating in the marketing sphere, these pending regulation changes don't have to be met with fear and should not be seen as a restrictions. Rather, marketers can use the steps for this much-needed revamp in responsible marketing - to differentiate themselves as a company that is committed to a mutually beneficial customer relation and exchange of value. Our recommendations to clients are to:

- **Centralize using the most appropriate technology:** the challenge of multiple fragmented channels, platforms and databases within organizations means that companies need to centralize their approach to GDPR through data management technology;
- **Organize roles and permissions:** start to proactively manage consent and user roles within your organization using a basic framework as a starting point, identifying who has access to what, and when?
- **Recognize opportunities to orchestrate:** using a central command center for cross-channel outreach, businesses can increase their understanding of a customer's profile while, responsibly, balancing one-to-one personalization with uncompromising protection;
- **Flexibly differentiate:** it follows that GDPR should not hinder but enable marketing to adapt, adopt, test and learn keeping pace with the fast-evolving world of their customers.

7. Why Capgemini and Relay42?

Capgemini and Relay42 have partnered to provide a carefully balanced suite of solutions to help marketing departments take advantage of the opportunities offered by GDPR.

- Capgemini offers extensive solutions in both process organization and IT solutions to help you get ready for the impending regulatory changes;
- Capgemini can carry out a PIA to assess your company's maturity in terms of readiness;
- Capgemini can assist customers in the development of the appropriate "skillset", including the start-up mentality that can take your company to the next level of customer trust and regulatory compliance;
- Relay42 provides advanced data management solutions that can help turn a centralized marketing framework into technical reality;
- Together Capgemini and Relay42 work with enterprises to help empower them to become customer-centric at scale, through modulated and secure technology, and responsible and responsive strategy. While Capgemini contributes insight, advice and consulting, Relay42 offers enterprise software for the CMO to orchestrate agile, one-to-one marketing at scale, and with consistent results.

8. About the Survey

Censuswide, an independent market research firm, was commissioned by Relay42 to undertake the survey during May 2017. 50 interviews were conducted using an online methodology across C-Level executives within the Financial Services Industry in the United Kingdom. Quotas were placed on age, gender and region across each market to ensure a nationally representative audience.

Accreditation: Censuswide.com complies with the MRS Code of Conduct (2014), which is based upon the ESOMAR principles (for more information visit *www.esomar.org*).

9. References

1. Loic Triger, TechRadar, December 2014

2. Jeroen van Zeeland, Capgemini, Relay42, April 2017, How Relay42 Helps Marketing to Remain GDPR Compliant

3. Christer Jansson, Capgemini, February 2017

4. Maxwell Keyte, Capgemini, Franck Hourdin, Oracle, 2017

5. Erik Matlick, Martech Today, June 2016

6. Capgemini The Currency of Trust, Why Banks and Insurers Must Make Customer Data Safer and More Secure, January 2017

i Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.

ii In cryptography, a salt is random data that is used as an additional input to a one-way function that “hashes” a password or passphrase. Salts are closely related to the concept of nonce.

Find out more

Want to further explore how you can turn GDPR from a threat into an opportunity with DMP technology, industry insights or a GDPR readiness assessment? We can provide a half-day workshop to help decide your next GDPR steps, carry out a PIA assessment, or explore for example a more layered approach to consent management using our GDPR consent management template.

For more details contact:

Jeroen van Zeeland
Real-time Dialogue Framework and CVA, Capgemini
jeroen.van.zeeland@capgemini.com

Julius Abensur
Financial Services Director, Relay42
j.abensur@relay42.com

Ron Tolido
Global CTO Insights & Data Global Practice, Capgemini
ron.tolido@capgemini.com

About Relay42

Relay42 is an enterprise Data Management Platform (DMP) empowering brands to turn their marketing into human dialogue. By unifying every consumer channel quickly, marketers can plug-and-play, personalizing every piece of outreach for the right message, to the right person, in the right context.

Protecting customer data - your vision, our vision:

At Relay42, we believe that the GDPR presents an opportunity for businesses to add value through responsible marketing. Using flexible and nuanced data management technology to unify disparate data sources, means marketers can control the orchestration of customer data and manage consent on multiple levels, and from a central location.

Learn more at
www.relay42.com

About Capgemini

With more than 190,000 people, Capgemini is present in over 40 countries and celebrates its 50th Anniversary year in 2017. A global leader in consulting, technology and outsourcing services, the Group reported 2016 global revenues of EUR 12.5 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at
www.capgemini.com