WHITEPAPER

GDPR

How GDPR Will Change Your Contact Centre.

T +632 849-3954 **E** info@ipintegration.ph **W** www.ipintegration.ph

DELIVERING BEYOND TODAY.

WHY NEW REGULATION IS TIMELY

The General Data Protection Regulation (GDPR) has good reason to exist.

The world is a different place since the first generation of data protection legislation that evolved during the 1980s-90s. We are now in a highly-connected world brimming with ambition to go much further.

Consumers continue to set the pace with their rapid adoption of new digital behaviours. Organisations are trying to keep up, aware that they need to balance expectations for real-time personalised engagement while also being sensitive to consumer concerns over privacy and ID theft.

It is therefore no surprise that legislation is in constant catch up. Both the E.U.'s intent to harmonise data laws across member states and the U.K. government's launch of a national cybercrime strategy are part of the same effort to keep pace.

The former requires organisations to step up their efforts in ensuring the data held on their customers is responsibly and securely managed. The latter tackles the broader issue of containing the ever-growing tide of online criminal activity. Acting in the way GDPR envisages will become a crucial deterrent against cybercrime - a challenge all contact centres face.

It is clear that things have changed so fast, that the majority of us are unaware of how our personal data is now collected and used. Traditionally, it was collected directly from us, for example when we filled in a form. Increasingly, organisations use data that we have not consciously provided.

For instance, personal data may be:

- Observed by tracking consumer behavior online or by smart devices
- Derived from combining other data sets
- Inferred by using algorithms to analyse a variety of data, such as social media, location data and records of purchases to profile us in terms of our credit risk, state of health or suitability for a job

Each of the above is considered a type of "processing" of personal data, subject to GDPR. While in the best cases, these techniques can be used to deliver shared value to both organisation and customer, the GDPR aims to rebalance matters.

GDPR sets new standards around your obligations as an organisation while empowering individuals with greater control and more rights in how their personal data is managed. Getting to the essence of the GDPR requires a mindset change for many U.S. businesses. Organisations should no longer imagine that they own their customers' personal data. They have it on loan. And so need to earn their customers' trust if they wish to retain access to it.

The GDPR is a legal framework for handling personal data of individuals based in the E.U., wherever in the world their data ends up being held or used.

This whitepaper explores the likely impact the GDPR will have on your contact centre(s) and what you should be concentrating on between now and when it comes into law in the United Kingdom from 25th May 2018. You should be prepared to re-assess everything from traditional working practices to the impact of using the newer digital services such as profiling previously mentioned.

ONGOING DEVELOPMENTS

Many of the GDPR's concepts and principles are much the same as those in the current UK Data Protection Act (DPA). However, there are new elements and significant enhancements, so you will have to do some things for the first time and some processes may change.

Since this is E.U. regulation, the prospect of Brexit raises an obvious question. Will GDPR still apply? As Brexit is unlikely to have been completed by May 2018 (when GDPR takes effect), GDPR will likely take effect in the U.K.. In addition, both the U.K. government and Information Commissioner's Office (ICO) have confirmed that GDPR remains the intended post-Brexit U.K. standard for data protection and will replace the DPA.

While the 219-page regulation is already published, there is still plenty of detail to iron out. This is being tackled by an E.U. wide group of data protection (DP) authorities who operate under the catchy title of 'Article 29 Working Party'! It is their job to keep providing detailed guidance on how to implement the regulation.

The ICO, as a data protection authority, is the most important voice from a U.K. perspective on the priorities and implications of the GDPR. You can sign-up for their newsletter at ico.org.uk. and stay current as things progress.

As far as your own contact centre efforts are concerned, be aware that you will need to consider an organisational-wide response. This might be coordinated by a cross functional team and maybe even headed up by a Data Protection Officer, which many organisations will be required to appoint and who will become responsible for your ongoing compliance.

However, even in organisations that have now received executive attention and sufficient funding to prepare for GDPR in time, every effort still makes a difference. Offering your own expert insight into the issues that customer service and contact centres are going to face while becoming GDPR compliant will be a great contribution and help build momentum towards the right outcomes. This is regulation for which everyone, including sole traders, startups, small to medium organisations, and large organisations, needs to prepare.

ONGOING DEVELOPMENTS

GDPR legal expert Chiara Rustici makes clear in her latest book on the topic just how wide the net is being cast. She clarifies that GDPR protection of someone's personal data is triggered by that person's physical location in the EU, not by their nationality.

> "It is the physical presence in the E.U. either of the individual or of the individual's data that triggers their GDPR data protection rights."

And GDPR data protection rights apply even if their personal data is being stored and processed outside the E.U. However, as Chiara Rustici goes on to explain, this is going to require considerable unpicking for some organisations.

> "Lack of visibility of digital data flows becomes a GDPR liability when personal data, or personally identifiable information, is scattered among the rest of a business's corporate data and bundled off to unidentifiable server farms."

Individuals also remain GDPR protected if they temporarily or permanently leave E.U. territory providing their data is still physically held within the E.U. So too would be visitors to the E.U. who become your customers during their stay. [1]

This is a broad net, and there is a lot to chew on in terms of customer engagement. Obviously, most scenarios include GDPR compliance. For instance, U.K. businesses processing personal data for partners in the E.U. would also be in scope.

WHY DOES THE GDPR MATTER?

Under the existing data protection regime, the ICO could only fine organisations up to £500,000 for the most serious data breaches. As such, it was possible to consider these as a cost of doing business. The GDPR raises the stakes to a whole new level.

Under GDPR, the maximum fine is now up to 4% of a group's global sales or 20 million Euros, whichever is higher. Even if a subsidiary is found in breach of the GDPR, the whole group's worldwide sales are used to calculate the potential fine.

To put that into context Talk Talk's £400,000 fine for their 2015 data breach would rise to around £72 million.[2]

In terms of further consequences, organisations are also exposed to the possibility of further consumer litigation. If PCI claims are any example, this could attract both privacy activists launching class action style lawsuits and firms seeking a 'no win, no fee' revenue opportunity.

Beyond any direct financial impact is the prospect of reputational damage. A 2016 global survey of 9,000 consumers showed 70%

believe responsibility for protecting personal data lies with organisations. Yet just 29% believe companies are taking protection of their personal data very seriously.[3]

In summary, the mismanagement of customer data really matters, both to the bottom line and to your brand's reputation. The GDPR legal framework reflects the urgency required to deal with an issue that currently threatens to undermine the digital economy. More than 4.8 billion data records have been exposed since 2013 with identity theft being the leading type of data breach accounting for 64% of all data breaches.4

Unlike previous generations of data legislation, the consequences of being part of the problem can no longer be counted as the cost of doing business. And as a major touch point, the contact centre is right in the thick of it.

KEY POINTS IN THE GDPR & IMPLICATIONS FOR CONTACT CENTRES

Before we summarise what the GDPR covers, it helps to understand some of the core thinking behind it.

The first idea is that there are two separate things the GDPR seeks to protect - the individual and their personal data. Consumers are being protected in their right to privacy. They can also expect their data to be protected. Understanding this explains why certain rights exists as we are about to explore.

Secondly, the GDPR categorises organisations in one of two roles: as controller or processor of personal data. Put simply, controllers are primarily responsible for ensuring data is collected and processed in compliance with GDPR, and ensuring data subject rights are complied with. Processors are also directly liable for compliance with certain obligations under GDPR, including ensuring security and confidentiality, and are expected to cooperate with controllers to ensure their compliance with requirements, obligations, and restrictions under GDPR. Processors are also subject to significant fines for GDPR violations. This has significant implications for those offering contact centre services.

Thirdly, the GDPR demands a certain level of ongoing data management competency. This requires organisations to provide evidence of how customer data is being used, and where it is being stored and processed at any given point in time. Think laptops being taken home at night or smart phones being lost. What about the way certain cloud services store data across multiple locations? Do you have strategic partners who incorporate this into their solutions? In this respect has working from home or remotely suddenly become a problem? There are many angles to consider.

A core principle of data protection is that personal data must be processed fairly and lawfully. So being transparent by providing a privacy notice is an important part of fair processing. In addition, organisations must have a valid legal basis, such as explicit consent, for processing personal data regardless of whether their privacy notice is appropriate and adequate. GDPR sets forth detailed requirements for both privacy notice and consent, which must be met for these to be effective from a GDPR perspective.

Finally, the rights of children are given prominence in the sense that their need for privacy and protection is all the greater in today's online world. So for instance, workflows around children's consent need to be carefully designed to ensure they are aware of what they are signing up for and its consequences. The right to remove their data also requires special attention in terms of making it easy and fast.

These scenarios provide a snapshot of the significant planning that is required from a compliance program perspective. They matter even more in the event of an investigated breach and how the ICO then evaluates the size of any fine. Incompetence in basic personal data management is likely to result in more severe penalties.

THESE ARE THE KEY POINTS IN THE REGULATION

Accountability & governance. You must practically demonstrate your accountability and governance strategy for protecting an individual's privacy and personal data.

- Contact centre implications In step with other leaders within your organisation, you will need to resource activities such as GDPR induction awareness, staff training, maintaining relevant documentation of processing activities and conducting internal audits. If you are so minded, fully embracing the customer interests at the heart of the GDPR also suggests that total team involvement is better than just command control compliance.

Right to information and transparency. Controllers are required to inform individuals about the purpose and basis for the processing of their personal data, the intended retention period, any non-E.U. storage and processing, the right to withdraw their consent anytime, the right to file a complaint, any use of automated decision making and how data about them is sourced. Usually this will be communicated in the form of a much more detailed privacy notice than is the current norm.

- Contact centre implications Since retention periods are based on intended use, do your live assistance/self-service resources need to recognise this and then respond appropriately (for example, when onboarding a new customer)? Equally, what workflow adaptations are needed to correctly record and route any requests to withdraw or complain that flow through the contact centre?

Right of access. Individuals can make reasonable requests to access their personal data, this time without cost. Information must be provided without delay and at the latest within one month.

- Contact centre implications Self-service is often the most consumer-friendly approach. Can your contact centre use whatever self service capability it has to enable this? Or is this a great excuse to upgrade?

Right to change inaccurate data. Individuals are entitled to have personal data updated if it is inaccurate or incomplete within a month of making the request. If you have disclosed the personal data in question to third parties, you must inform them of the correct details where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

- Contact centre implications Can this be incorporated into an interactive self service capability so that customers can edit their own data? How will you ensure that any third parties e.g. BPO partners or list brokers are informed of these changes and update their own records?

THESE ARE THE KEY POINTS IN THE REGULATION

Right to object. Individuals have a right to object to automated decision making (profiling) and direct marketing.

- Contact centre implications How are advisors empowered to satisfy the requirement that individuals can challenge automated decisions which negatively impact them such as decisions around lending, mortgages, insurance etc.? Specifically, customer rights need to be clearly explained to them and then fulfilled in terms of:

  - Offering human intervention
  - Allowing them to express their point of view
  - Offering an explanation of the decision and allowing it to be challenged

Right to data portability. Individuals can, under certain circumstances, request a copy of their data in a structured, digital, and commonly used format from the controller. This helps them move their business to another supplier.

- Contact centre implications How will you process this type of request? Is it important that advisors or self-service channels have the ability to check on the status of any such requests?

GDPR accredited. Organisations can only use contractors and subcontractors that comply with applicable GDPR requirements. The ICO encourages industry sectors to create codes of conduct which they will then approve as a way of recognising competence. Nothing as of yet has been published for the contact centre industry.

- Contact centre implications Data controllers are legally liable for all other controllers and processors included in your 'value chain'. This could include BPO partners, list providers, infrastructure providers especially cloud vendors processing or storing customer data within CRM, CTI or PCI solutions or 3rd party specialist data services. You are accountable for any breaches they cause.

  - How will this change the way you choose and verify they are and remain GDPR compliant?
  - How is GDPR compliance reconfirmed across your value chain when things change such as new campaigns, infrastructure upgrades and product launches?
  - In turn, your value chain partners are under an equivalent requirement to refuse any instruction from you that is non GDPR compliant. How do you ensure this is heard and acted on?

CONCLUDING THOUGHTS

GDPR changes the way organisations and their customers engage. Its impact will be to improve the standards around privacy and data protection. Those that succeed can expect greater trust from their customers as a result. As we said at the beginning of this whitepaper, this is the direction of travel for today's digital economy. However, as GDPR has recognised, before that can happen, standards must improve. Moreover, the ever-growing threat of cybercrime must be reduced if a digital economy is to remain viable.

Contact centres are involved in many respects.

In terms of cybercrime they remain a vulnerable touch point. Social engineering is always going to be an issue when people are involved, especially when we expect contact centres to be open to customer needs and orientated to deliver great experiences. Dishonest employees remain another concern. Positive and inclusive cultures can certainly help reduce grievance based

dishonesty. Meanwhile, proactive governance must become effective enough to help spot those that mean us harm regardless. All of this implies that GPDR has to become part of the daily workload as opposed to a one off or occasional exercise.

Self-service technologies such as IVRs have proved another weak link in the security chain. Maybe it is only a matter of time before intelligent assistants fall prey to similar fraudulent efforts. GPDR penalties mean much greater effort to prevent this must become a top priority.

Customers will also engage with our contact centres around many of the rights that GDPR define. The role played by the contact centre in meeting GDPR requirements will have to be part of a coordinated organisation wide response. The ability to track and care for customer privacy and personal data across their lifecycle provides yet another reason why marketing, sales and service teams should be moving towards deeper collaboration.

Preparedness requires a strategic change management plan including an upgrade of skills, new policies, workflows and roles. Technology has a vital role to play in the governance and management of these requirements. Much of what is currently used in contact centres will need to be upgraded to become GDPR compliant.

In particular, contact centres need to use technology to move onto the front foot in terms of responsiveness. The vast majority of large scale centres rely heavily on live assistance and the voice channel in particular. Therefore, the voiceprint of fraudsters needs to be recognised and responded to in as near real time as possible.

As previously mentioned, social engineering will always be a point of attack especially for centres still reliant on less than effective protocols such as knowledge based identification and verification. IVR will also need to be scrutinized, having proved to be an effective hiding place to run multiple sessions to break into user accounts. Technology exists to counteract each of these threats.

In the U.K., the way in which the ICO acts as educator, interpreter and enforcer will be key to the way GDPR rolls out, as will the way in which executive teams decide to craft their GDPR strategy. Some will play close to the wind. Others will use it as a way to advance their customer engagement agenda by meeting these core customer expectations.

Consumers appear to welcome GDPR. "81% are forecasting they will become more likely to share their personal data once GDPR is in place".[5]

This gives us a glimpse of the upside GDPR offers for organisations and their customers. Meanwhile, we wish you well in all your preparations and hope this whitepaper has helped you on that journey.

Source's:

1 GDPR- The Functional Specifications of E.U.-Grade Privacy
2 Keynote presentation from André Bywater, Partner, Cordery at Customer Data Security Conference February 2017 London.
3 Gemalto's 2016 Data Breaches and Customer Loyalty 2016 report.
4 Gemalto's H1 2016 Breach Level Index
5 Unlocking The Potential Of Personal Data. Callcredit Information Group 2016

CHANGE TODAY AND YOU CHANGE TOMORROW

The way we communicate continues to change at pace. Tomorrow has never looked so different from today. IPI is here to keep your business in touch with its customers.

With innovation in our DNA, we deploy pioneering solutions to help create the smartest, most efficient Contact Centres in the world. Optimised hubs that offer a more satisfying, more cost-effective customer experience.

And just as our offering is complete, so too is our support. Helping you to not just prepare for what's to come, but to embrace it.

Headquartered in Reading, and with offices in Manchester and Edinburgh, IP Integration is a leading independent contact centre systems integrator. We partner with many leading vendors, including Avaya, Verint, Microsoft and VMware. We also develop in-house bespoke applications that support end-to-end contact centre deployments, from network service provision, through systems design and deployment, to application development and post-implementation service and support.

Our team of experts understands the technical, commercial and organisational challenges contact centres face and offers a wide range of solutions that help organisations overcome them to increase effectiveness, efficiency and customer satisfaction.

Our customers range in size from 30 to 10,000 seats, such is the flexibility and scalability of our solutions, and are split across many vertical markets including finance, insurance, retail and distribution, public sector, transport and travel, and entertainment and leisure. In addition, IP Integration meets BSI standards in Quality Management, Environmental Management and Information Security Management.

Change your tomorrow, today. Get in touch.

T +632 849-3954 **E** info@ipintegration.ph **W** www.ipintegration.ph

DELIVERING BEYOND TODAY.