pindrop
WHITE PAPER

General Data Protection Regulation (GDPR) Impact on Contact Centres

The European Union's Advanced Directive for the Protection of Personal Data

The GDPR went into effective on May 25, 2018, changing how all organisations manage the personal data of EU residents.

In response to the growing threat of security breaches, countries across the European Union (EU) have enacted stringent legislation and regulation regarding the protection of personal data. To maximise protection, the EU replaced the Data Protection Directive (DPD), which previously regulated the processing and free movement of data within the entirety of the EU, with the General Data Protection Regulation (GDPR). The GDPR went into effect May 25, 2018, changing how all organisations manage the personal data of EU residents.

Contact Centres & Data Protection

The European Commission defines personal data as "any information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking information, medical information, or a computer IP address."

In looking at GDPR compliance, organizations will need to focus on the vulnerabilities of all communication channels, particularly the phone channel, where personal data is constantly collected and processed. Personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" (GDPR, Article 5). In order to uphold the requirements of the GDPR, contact centres, which are particularly susceptible to personal data breaches, must be able to accurately authenticate a caller before granting access to personal data, and this is often where the struggle lies.

Non-compliance with the requirements of the GDPR may result in:

- A written warning in a first case of unintentional non-compliance
- Regular periodic data protection audits
- A fine of up to €20M or 4% of the preceding financial year's annual worldwide turnover, whichever is greater

Contact centres are ideal targets due to:

Valuable Data.

The wealth of information housed by contact centres can be leveraged by fraudsters for data mining and attacks in other channels. Interactive Voice Response (IVR), often unprotected, also gives fraudsters the opportunity to collect data, and forms of Knowledge-Based Authentication (KBAs) are easily hacked due to information gathered from these data breaches.

Lack of Security.

Unprotected contact centres are ideal targets for fraudsters due to numerous vulnerabilities. The contact centre requires multi-layered security in order to successfully combat these attacks.

Cross-Channel Enablement.

Although these attacks may not lead to account takeover immediately, omnichannel data mining can contribute to fraud at a later time. The contact centre enables cross-channel fraud attacks, making it difficult for organisations to diagnose the source of a data breach.

Social Engineering.

Pressure for agents to deliver the highest quality customer experience along with lack of training on how to identify fraud attempts makes

them more vulnerable to fraud. Through psychological manipulation, these agents unknowingly enable fraudsters by performing certain actions or divulging confidential information.

Fraud Technology. Readily available fraud technology (i.e. spoofing, voice distortion, VoIP, etc.) makes it easy for fraudsters to impersonate legitimate callers and opens the door to data breaches.

Protecting Personal Data in the Contact Centre

Under the GDPR, contact centres now hold immense responsibility and accountability regarding the protection of personal data. Because individuals now have the right to access, obtain, change, and erase personal data held by organisations through the GDPR, it is necessary for contact centres to ensure that the personal data they house is only made accessible to the legitimate customer. Data protection needs to be incorporated into all business processes, products, and services, ensuring that all employees of an organisation are aware of their obligations to protect any personal data to which they have access.

Pindrop's Recommended Multi-Layer Approach

If one layer of security is compromised, all channels are vulnerable. In order to protect client data and avoid the threat of account takeover, Pindrop recommends contact centres to employ a security solution that provides:

Universal Coverage. Customers must be authenticated and fraudsters must be identified on their first call. This prevents fraudsters from being able to enroll as illegitimate customers and alleviates customer privacy concerns.

Accuracy. The right solution accurately differentiates between legitimate and illegitimate customers. Legacy solutions, such as Caller ID verification and KBA, fail to provide the accuracy needed.

Speed. Contact centre agents must be informed about the legitimacy of callers before they provide access to personal data. KBA takes a long time, which frustrates legitimate customers and offers fraudsters many chances to collect data.

Low Friction. Customers want service that requires little effort on their part. Most voice biometrics solutions require an enrollment process, which leads to longer call times and lower customer satisfaction.

Not Easily Fooled Technology. Fraudsters are currently using voice distortion, spoofing, social engineering, gateway hacking, and more to circumvent traditional security measures. The right solution needs to withstand these attempts to break through protection.

Pindrop's technology solutions enable organisations with holistic, multi-layer security and defense mechanisms to help meet GDPR requirements. Pindrop protects the contact centre through:

Real-Time Risk Scoring. Pindrop's solution provides contact centres with a pop-up risk score for each incoming call in less than 30 seconds. This score directs contact centre agents to administer customised authentication methods to specific callers. For callers with a low risk score, contact centre agents can reduce call handle time, improving the customer's overall experience while reducing call centre costs for the organisation. For callers with a high risk score, contact centre agents know to provide additional security by stepping up authentication methods in order to ensure a caller's identity.

Fraud Detection. Pindrop's fraud alert system combines sophisticated audio analysis through Phoneprinting technology based off of reputation, network, behaviour, and statistics. This system identifies risky callers for contact centre agents so that they don't fall victim to social engineering tactics and fraud technology. Suspicious callers are flagged and routed, prompting additional investigation in order to prevent loss. High-risk callers are flagged and blacklisted, ending the potential for future loss.

Case Manager. Case Manager is a web-based tool for an organisation's contact centre technologists and fraud analysts to investigate potential data breaches. Through on-demand call playback, advanced machine learning, and analytics, fraud teams can effectively identify and predict fraudulent activity. Pindrop's Case Manager allows users to easily manage call data and investigation activities, dramatically increasing productivity for an organisation.

Pindrop's technology provides verifiable support that an organisation is processing calls with a high level of protection, therefore better aligning with GDPR's protocols. Today, many of the world's largest enterprise contact centres are using Phoneprinting™to protect customers and deter fraud, while reducing costs and improving customer experience. Customers are enabled to catch over 80% of fraud calls with less than a 1% false positive rate.