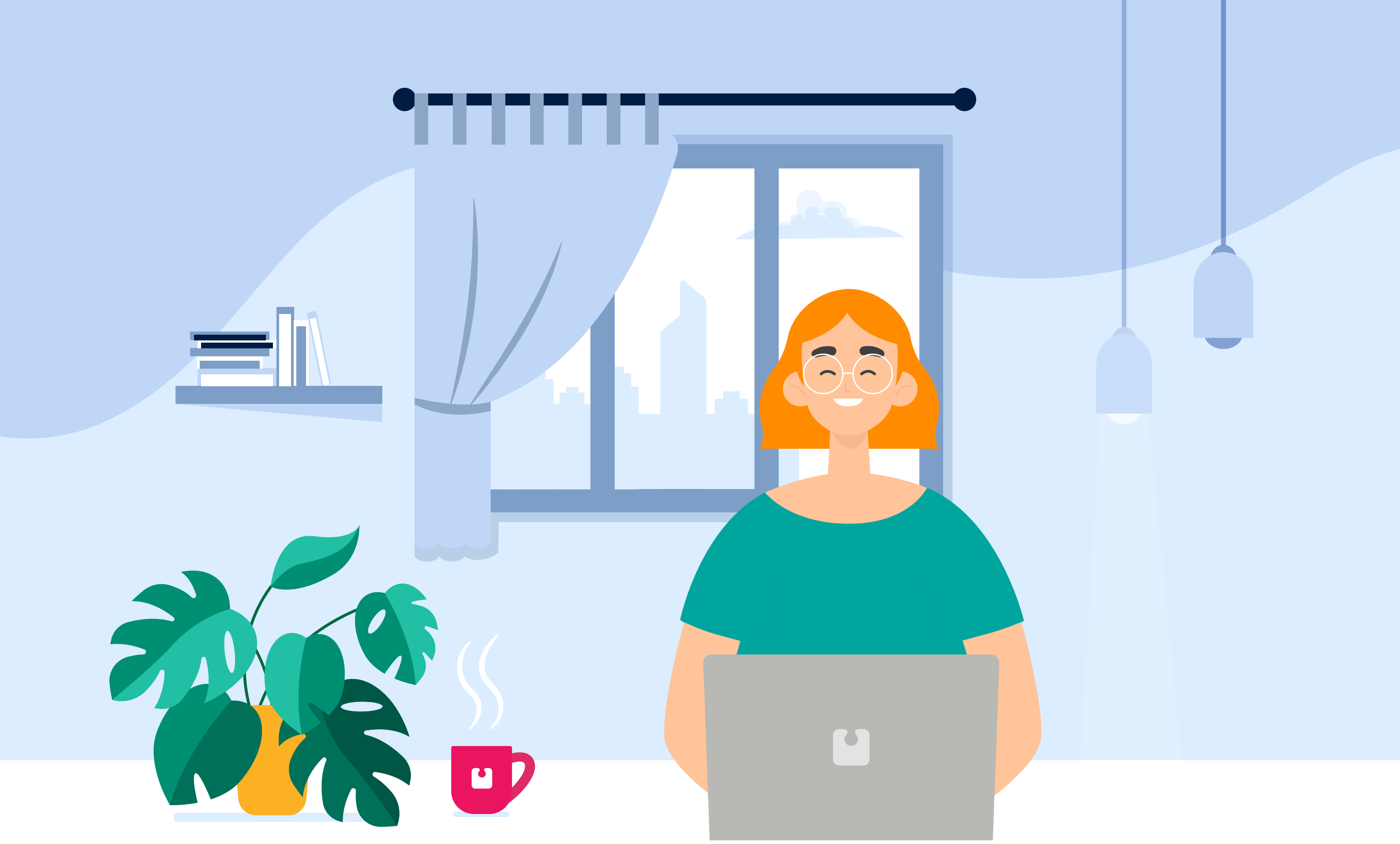
Securing your contact centre

puzzel. Solving Customer Interactions

puzzel.com



Introduction

Security threats have escalated during the Covid-19 pandemic.

Many organisations were not prepared for remote working when lockdowns were announced in 2020 and had to implement quick-fix solutions to enable their staff to work from home. This has led to a rise in cyber crime and data breaches, which can have severe consequences for companies, employees and customers.

Contact centres are prime targets for cyber criminals due to the high volume of customer data that is transacted every day. So how you can boost security, maintain data protection and safeguard your employees from fraud during these exceptional times?

This white paper will explain the different types of data that a contact centre typically manages and how these can be protected. It will also explain the importance of access management and the data protection measures that Puzzel has implemented to comply with GDPR. Finally, it will share three basic security measures that contact centres can implement right now to reduce their vulnerability to fraud.

Data classification and information flow

Contact centres process a high volume of communication data through interactions with customers. This communication data can be divided into two main categories:

Electronic communications metadata

Electronic communications metadata refers to the information connected to communications that does not include the content. This can include email addresses, phone numbers, timestamps and the names of contact centre agents involved in interactions.

Electronic communications data

Electronic communications data refers to the content that is transmitted or exchanged. This is the information recorded in web chat transcripts, call recordings or voice transcripts, SMSs, emails and attachments.

Both electronic communications metadata and data can contain sensitive personal information related to your agents and customers. For example, if you provide health services and have enabled call recording, there's a chance that those recordings will contain sensitive personal data about your customers' health.

Puzzel's cloud contact centre solution can process enquiries from all different channels, including voice, social media, email, web chat, and SMS. All data flows securely through the platform and is stored in each of our customers' own contact centre solutions. This means it is isolated to the customer only and is fully under their control.

Access management

Access management is crucial to ensuring the security of your contact centre.

If you are using a cloud contact centre solution, it is your responsibility to create your own users and assign access according to their needs. Puzzel customers have full control over managing their own users, user groups and corresponding profiles and settings. Our customers control access within their own contact centre solutions, with rights able to be configured right down to the smallest detail within the Puzzel Administration Portal.

To enable our customers to have full control over their contact centre, Puzzel has implemented customer specific logs that record the customer's own activity within their service. Three types of logs have been implemented:

1. The **Access Log**, which details successful and unsuccessful login attempts, who has logged on and when

2. The **Puzzel Archive**, which contains information about all interactions and corresponding recordings and chat transcripts. This includes information about who has accessed, listened to and/or downloaded a call recording or chat transcript and when

3. A **Change Log**, which records who has changed what and when in your contact centre solution

Each of these logs can be restricted to individual users or groups. This enables our customers to have a thorough overview of what is happening within their contact centre. They can also fetch these logs through Puzzel's API and then import them into their own security monitoring solution for central management.

Top tip: If you use single sign-on, make sure you have implemented strong passwords, two-factor authentication and enabled regular password changes. Puzzel customers can enable these settings within the Puzzel Administration Portal.

GDPR and compliance

There are six data protection principles listed in Article 5 of the General Data Protection Regulation (GDPR).

Privacy by design and default involves adherence to these principles.

They are:

A) Data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. This is referred to as lawfulness, fairness and transparency. A data subject is a living person – the person who the information relates to. GDPR does not apply to deceased persons.

B) Data must be collected for a specific, explicit and legitimate purpose and not further processed in a manner incompatible with those purposes. This is referred to as purpose limitation.

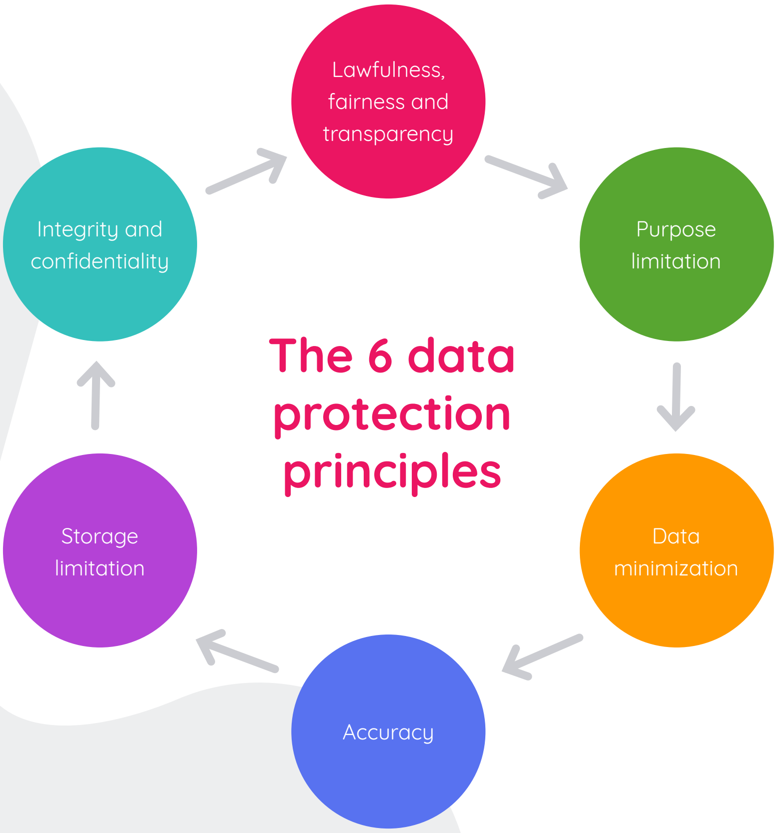
C) Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This is referred to as data minimisation.

D) Data must be accurate, and the necessary kept up to date, erased or rectified without undue delay. This is referred to as accuracy.

E) Personal data must not be stored for longer than its necessary purpose. This is referred to as storage limitation.

F) Organisations must ensure appropriate security of personal data, including protecting against unauthorised or unlawful processing and against accidental loss destruction or damage using appropriate technical and organisational measures. This is referred to as integrity and confidentiality.

Puzzel customers are responsible for their own compliance with these principles. But to be able to demonstrate compliance, Puzzel as a processor needs to support by providing compliant services.


Lawfulness, fairness and transparency
Purpose limitation
Data minimization
Accuracy
Storage limitation
Integrity and confidentiality
The 6 data protection principles

Here are the measures we have implemented to address each principle in the Puzzel Contact Centre:

Principle A: Lawfulness, fairness and transparency

Puzzel's privacy policy and data processing agreement is publicly available for our customers and their customers. Individuals have the right to request access to their data, rectify incorrect data, erase data when it's not needed anymore and to get a copy of their data when requested.

Principle B: Purpose limitation

Puzzel does not use customer data for testing or any other purposes than agreed.

Principle C: Data minimisation

Puzzel only collects the required information that is necessary for us to provide the services to our customers. All personal data is erased when its purpose has been fulfilled.

Principal D: Accuracy

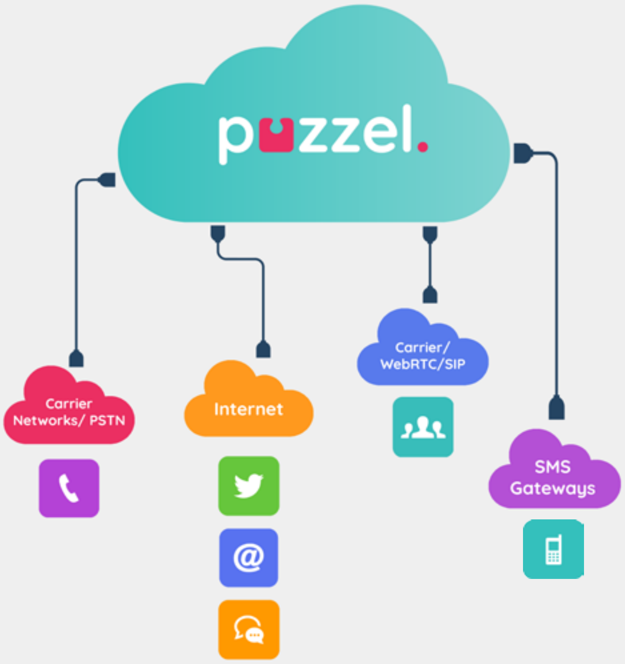
The nature of the services we provide ensures accuracy by automatic data collection. We have implemented self-service for our customers so they can update personal data where applicable and manually erase data when requested. In relation to access requests from individuals, our customers can serve these requests on their own by searching for, changing, deleting and downloading information directly in the Puzzel Administration Portal. Our customers do not need to involve Puzzel to secure compliance against those rights for the individuals.

Principle E: Storage limitation

Puzzel has implemented customer specific data retention schedules with automatic erasure of data every night. This means the Puzzel Contact Centre supports individual customers' needs for storage retention. We store the data according to our customers' or your requirements, so if you want to store the data for 12 months, that can be configured and data will then be automatically deleted accordingly.

Principle F: Integrity and confidentiality

Puzzel provides highly available services and has implemented several security measures, including redundant services, backup disaster recovery, secure communication and file transfer (referred to as encryption) and access control mechanisms. Logging enables our customers to audit access and built-in anonymisation enables our customers to anonymise a caller, chatter or an agent when required.



Technical and organisational measures

There are three basic security measures you can implement right now to significantly reduce the overall risk of your contact centre.

1. Awareness training

Awareness training will reduce the risk of successful fraud, phishing, malware, and ransomware attacks.

Email is involved in more than 90% of all network attacks. It is used to perpetrate fraud simply because it is hard to tell if an email is real. There are technical solutions you can implement to reduce the risk, but it's also important to educate your contact centre staff in how to identify email attacks and what to do when they receive one.

Contact centre agents are the front end or your organisation and are easy targets. You should also educate your staff in the importance of protecting their credentials.

2. Access control

Assign permissions to user groups within your contact centre solution and add users to these groups for easy management. You should require unique and strong passwords for all accounts and use two-factor authentication.

Two-factor authentication or multi-factor authentication is one of the single most effective controls to defend against security attacks.

3. Auditing

Disable or delete unused user accounts as soon as possible when people leave your organisation or are away for a long period of time. Audit access using the available logs and search for suspicious activities. Do you see a lot of unsuccessful logins? Maybe someone is trying to hack into an account? Talk to your users. Do you see any logons after office hours? Change the corresponding password for the account where you see suspicious activities.

All of these measures are easy to implement and will contribute to increasing the overall security of your contact centre and all other cloud applications.

It is also important that you ensure that your workers' devices are up to date to protect against known vulnerabilities. The Puzzel Contact Centre enables your agents to safely work from any location on any device, not only during these difficult times, but also in the future.

Next steps

To protect your organisation from cyber crime, you need a secure and compliant contact centre. Compliance is not only critical for remaining in business, but also for staying ahead of your competition and avoiding punitive sanctions.

At Puzzel, we provide services that help our customers comply with national and international law, as well as industry specific standards and requirements such as ISO standards and GDPR.

For more information on our customer service solutions, please **visit our website**. For more information regarding industry specific compliance, or other details not covered in this white paper, please **visit our Trust Centre** or get in touch with us at privacy@puzzel.com.

About Puzzel

Puzzel is the leading European Contact Centre as a Service (CCaaS) provider. Our award-winning Customer Service Platform consists of three fully integrated, cloud-based solutions, including an omnichannel and AI-enabled Contact Centre, advanced email and Ticketing and Workforce Management, which are easy to use, quick to set-up and scalable for contact centres of all sizes. Customers can also customise the platform with dozens of third-party integrations available through our Puzzel Marketplace.

Puzzel was recognised as a Challenger in the 2019 Gartner Magic Quadrant report for Contact Centre as a Service in Western Europe and ranked in the top three European CCaaS providers for 2020 by Frost & Sullivan. Based in Norway, and with offices across Scandinavia, Europe, the UK and Asia, we work with more than 1,000 customers across 40 different countries, helping businesses to achieve success beyond voice, connected experiences and empowered employees.

For more information, please visit **www.puzzel.com**.