csg

TOGETHER, YOU WIN.

INTERCONNECT FOR GDPR

STREAMLINING ONGOING COMPLIANCE TO GDPR WITH CSG INTERCONNECT

As of 25th May 2018, all organizations that collect and/or process personal data from EU residents must comply with GDPR (General Data Protection Regulation) irrespective of where they are located. GDPR requires Data Controllers and Data Processors to keep a record of their processing activities, including organizational and technical security measures used to protect data, descriptions of data processed, where shared or transferred and erasure thresholds, which must be made available to supervisory authorities/regulators.

CSG Interconnect offers proven, industry-standard capabilities that support the key requirements for maintaining GDPR compliance. With capabilities such as pseudonymization, security and logging operations for securing personal data, CSG is helping operators around the world quickly enable GDPR compliance to deliver a secure solution that is cost-effective over the long term as operators maintain their ongoing compliance obligations.

DEMONSTRABLE COMPLIANCE

Many BSS vendors are focusing on the protection of personal data from breaches, with solutions like data masking. While implementing appropriate security measures against breaches is crucial for a wholesale management system, communication service providers must consider many additional aspects for end-to-end compliance. Given this larger scope, service providers need to evaluate how to not only achieve fast compliance, but also approaches that are cost-effective over the longer term.

PROTECTION OF PERSONAL DATA

Personally identifiable information (PII) data that is processed and stored within CSG Interconnect is limited to phone numbers or IP addresses within the Event Detail Record's (EDR) A NUMBER and B NUMBER fields. Additionally, the Interconnect EDR file format provides user-defined fields, USER_DATA and USER_SUMMARIZATION, that allow mediated values (potentially PII) to be passed to and stored within the Interconnect priced record.

GDPR requires that Interconnect must provide the ability for access to such personal data to be controlled and audited.

PSEUDONYMIZATION AND ANONYMIZATION OF PERSONAL DATA

Facilitating the reconciliation of invoices will invariably require an operator's mediated EDR to contain the full A/B number, being personally identifiable information. Some operators, on the other hand, need only process and store a significant number of digits from the EDR A/B number data to reconcile invoices. In these circumstances, the data processed and stored within Interconnect is no longer personally identifiable information, therefore minimizing exposure to GDPR regulations from wholesale data streams (by number masking or truncation).

CSG Intermediate provides an optional feature to support the selective anonymization (number masking) of the EDR A/B number data to be passed to Interconnect. Deployment of this upstream solution would minimize GDPR compliance within Interconnect, as data passed within the EDR would no longer be personally identifiable.

Where the full A/B number is required, Interconnect supports user access controls on viewing such data. There are various options available to pseudonymize data by masking a configurable number of least significant digits from the mediated number, either through the Security Role features based on a user or through Reference Data Parameters.

CSG has the expertise to evaluate your requirements so that these features are enabled seamlessly and effectively while ensuring your GDPR compliance obligations.

USER ACCESS CONTROL

GDPR requires that wholesale billing systems must support comprehensive and fine-grained application user security to control access to personal data and logging. Applications must also track user access to personal data and support user monitoring for tracking access to personal data providing sufficient traceability to identify unique users.

CSG Interconnect Security-User and Role controls which users have access to screens where personal data is displayed. By default and to ensure GDPR compliance, users will no longer be permitted access to these screens unless explicitly granted. This rule will require Security Role Parameters to be evaluated and set for all users ensuring access to screens containing personal data items is restricted to only those with a business need.

USER ACCESS TRACKING

All user access to personal data stored in Interconnect is recorded to the Audit Log. By default, a log is created for all operations on personal data showing what data has been accessed, the action taken including before and after values and by which user.

Audit Log information is available from Interconnect for reporting, thus limiting the scope of a breach notification.

GDPR SUBJECT-ACCESS REQUESTS (SAR)

Under GDPR, data subjects have a right to access their personal data held by a controller (i.e. Specific A/B number EDRs stored within Interconnect). Controllers will need to respond to a subject-access request and potentially provide the data they are storing.

CSG Interconnect supports SARs by way of the EDR Extract function, which extracts EDR records into a CSV file using selection criteria. Specific A/B number personal data may be extracted.

Additionally, it is possible to extract data using a profile that masks the A/B number fields where the Reference Data Parameter has been set for Pseudonymization.

ADDITIONAL SERVICE OFFERINGS

CSG can provide the expertise to ensure you are GDPR compliant for CSG Interconnect:

- Training on product features to assist with GDPR compliance
- Audit processes ensuring GDPR compliance
- Configuration of Security Roles
- Configuration of Reference Data Parameters and SAR requirement parameters
- CSG Intermediate Anonymization of EDR Personally Identifiable Data passed to Interconnect

SUMMARY AND BENEFITS

Time-to-compliance is critical for GDPR since the regulations carry heavy financial penalties for non-compliance, for service providers both inside and outside the EU.

There are three critical aspects to enabling GDPR compliance within a wholesale business management solution and streamlining the compliance process:

- Logging operations on personal data
- User access control and tracking
- Breach protection

CSG offers proven, industry-standard capabilities that support the key requirements for maintaining GDPR compliance. We help operators around the world quickly enable GDPR compliance and secure personal data.

ABOUT CSG

CSG simplifies the complexity of business transformation in the digital age for the most respected communications, media and entertainment service providers worldwide. With over 35 years of experience, CSG delivers revenue management, customer experience and digital monetization solutions for every stage of the customer lifecycle. The company is the trusted partner driving digital transformation for leading global brands, including Arrow, AT&T, Bharti Airtel, Charter Communications, Comcast, DISH, Eastlink, iFlix, MTN, TalkTalk, Telefonica, Telstra and Verizon.

At CSG, we have one vision: flexible, seamless, limitless communications, information and content services for everyone. For more information, visit our website at csgi.com and follow us on LinkedIn, Twitter and Facebook.