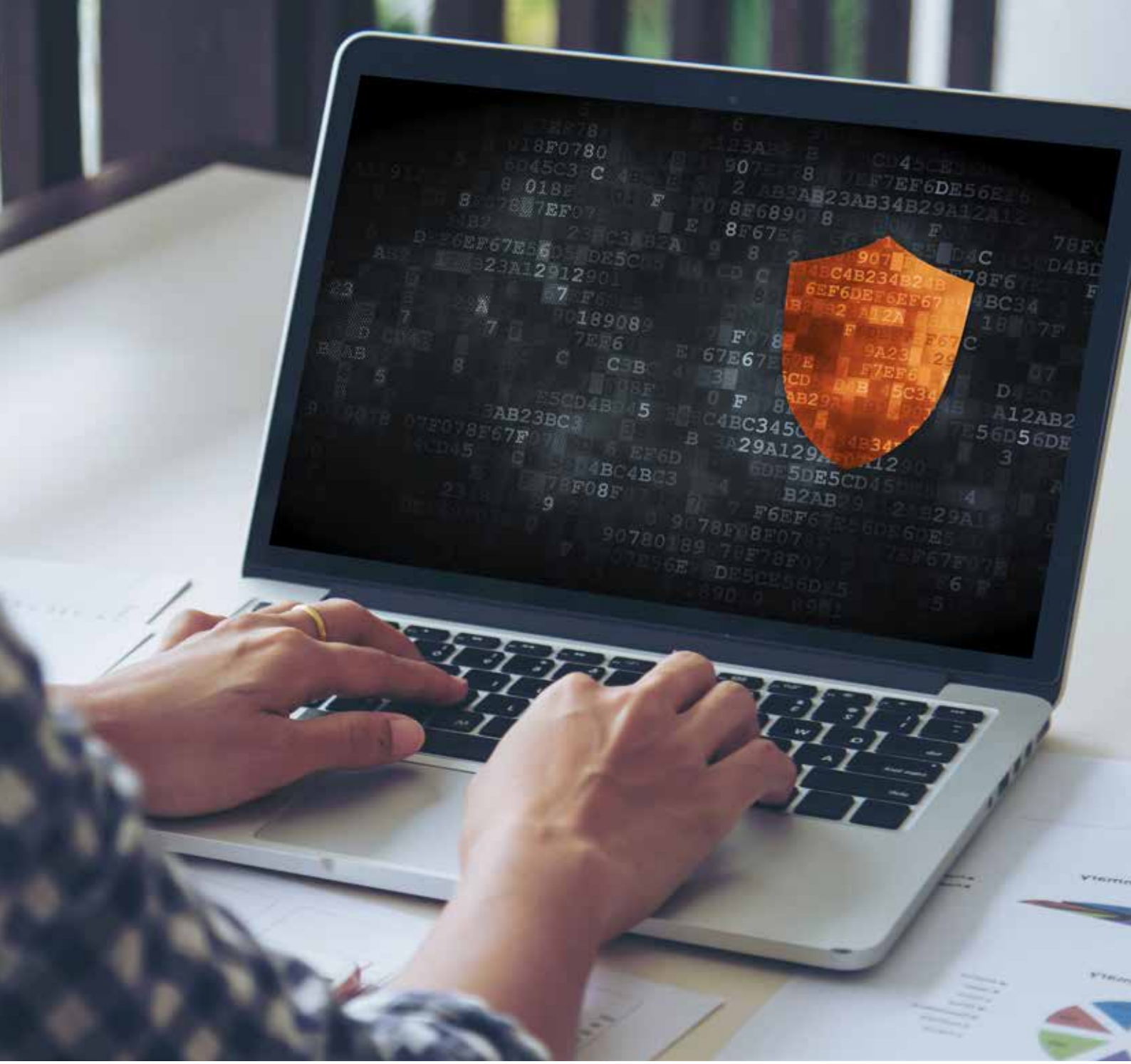

DATAFLOW

Information Security Compliance and Regulatory Adherence

The DataFlow Group takes data security and the management of Personally Identifiable Information (PII) seriously and has adopted a multi-faceted approach to ensuring it's safety, protection and restricted use. We constantly strive to protect the data asset's we are entrusted with and make use of a blend of traditional and emerging technologies to guarantee our services remain the best in the industry.

Discussed here are some of the more prevalent features pertaining to protecting the data we are entrusted with.

Audience and purpose

This document is provided to give an insight into how DataFlow manages data which it collects through its Primary Source Verification (PSV) process. Such data may be provided directly by the applicant, or provided via one of our client engagements.

In order for The DataFlow Group to maintain strict compliance with data regulations within the various countries in which it operates and processes applicant data, the document also outlines details of how the processing of data is undertaken and what rights an applicant may have over that data.

Data Management

Redundancy

Ensuring that our systems remain online and available when they are needed is critical to the services we provide. To that end, DataFlow has invested effort and money in providing a resilient architecture to host our core application for Primary Source Verification (PSV).

There are many layers in DataFlow's Core transactional system, VeriFlow, and all are implemented with multiple levels of redundancy to ensure maximum up-time for our internal processes. The design allows one or more elements to fail without any interruption in service by having multiple, redundant systems online to automatically assume processing on behalf of the failed component. Relying upon NetApp storage appliances and a virtualised server architecture on the industry-leading VMWare application, we commit internally to a 99.9% up-time of our services.

Likewise in our externally facing systems, DataFlow has taken the approach to virtualised environments one step further by instigating a program of change to move all external connectivity to Amazon's AWS architecture.

Using scale-on-demand services and in-built redundancy and elasticity, we feel we are moving towards an even more robust architecture and an "'always on" vision which will surpass our current external commitment of 99.9% up-time.

Disaster Recovery

IT Disaster Recovery (DR) and Business Continuity plans are designed to ensure continuity of critical business services with minimal disruption in the event of an emergency or disaster situation and are approved by the Corporate Executive group of Dataflow Group.

Our core transactional system, VeriFlow, is hosted on it's own equipment in a data centre provided by Tata Communications Limited (Tata). Data is replicated to a secondary appliance within the data centre and then to a tertiary cloud recovery service. In the event that the entire data centre fails, all operations fail over to the DR cloud layer. This failover procedure is tested and proven on the live site on an annual basis. Dataflow Group conducts annual DR exercises to ensure that systems and processes are in place, as well as to assess and enhance competency of all relevant personnel key to the successful implementation of DR activities.

Quarterly restoration of critical applications and databases are performed to ensure backups taken are effective and data can be restored within a REcovery Time Objective (RTO) of 24 hours in the event of an emergency or disaster situation.

Scalability

The DataFlow Group undertakes hundreds of thousands of compliance screening and verification service transactions for professionals each year on behalf of various government, quasi-government, regulatory and large multinational organisations worldwide.

DataFlow Group utilises cutting-edge technologies and leverages an expansive network of over 60,000 issuing authorities throughout more than 185 countries and territories to liaise with primary sources and verify the authenticity of documents submitted by candidates, in accordance with global industry best practices and Joint Commission International (JCI) guidelines. Dataflow Group has designed its systems to accommodate surges and spikes in usage, and to scale upward smoothly to address increased volume and transactions.

Data Storage

DataFlow makes use of several industry standard vendors in order to store data including:

Location: Global

Google

DataFlow uses Google for storage of it's own corporate data, and for email*. As a true cloud-based service, DataFlow data is hosted in a number of locations not known to DataFlow and is known only to Google. This forms part of their data redundancy and security model.

Location: Ireland

For our core transaction processing systems, we utilise large scale components from Amazon cloud services such as their storage, compute and database services. Data is stored on these devices in accordance with our retention policies.

Primary communication through our externally facing portals and our API services utilise Amazon's Ireland location for these cloud services. The data for case processing is Data is viewed from our sub-processing offices in Jordan, UAE, India and the Philippines.

Who we share personal data with

As part of our processes, and with the applicant's explicit written permission, we share a copy of the applicant's information with the Issuing Authority (the primary source) from where the information provided by the applicant originated.

On occasion, a third-party may be involved to obtain verified credentials. In this case, such business partners are contractually engaged with DataFlow to ensure that electronic and physical records of the data are deleted after completion of the verification request.

Application Security

Encryption & Hashing

Transmission of the user's unique ID and passwords, as well as all data in the resultant connection, are encrypted with industry standard protocol and cipher suite. Passwords are hashed using a strong SHA-256 hashing algorithm when stored in database.

Application-Only Access

The system is divided into layers that separate data from the application itself. Users of the application can only access the application features, and not the underlying database or other infrastructure components. Direct access to the database is restricted to database administrators and is provisioned on an as-needed basis with unique IDs.

Role-Level Access

Each end user is assigned a specific role with specific permissions to only see and use those features within the application which are related to his or her own job.

DATAFLOW

Audit Trail, Idle Disconnect & URL Tampering

There is a complete audit trail whereby changes to each transaction are tracked by the user login details and a timestamp for each change is provided. The system also detects idle connections and automatically logs out the user after a predefined time interval. User account is locked in case of URL tampering.

IP Address Restrictions

Access to the VeriFlow application from specific IP addresses is enforced. This feature significantly reduces the risk of unauthorized third parties accessing a user's personal data.

Robust Password Policies

Strong passwords configurations are enforced in line with global best practices such as minimum password length, password complexity, account lockout post failed attempts and password ageing.

Operational Security

Continuous Monitoring

DataFlow Group has configured its firewalls to detect and prevent intrusion activities. Unauthorised attempts to access the data center are blocked, and any unauthorised connection attempts are logged and investigated. Enterprise-grade antivirus software is in place to guard against Trojans, worms, viruses and other malware from affecting the corporate software and applications, and DataFlow makes use of keystroke logging and auditing software on all of its end-points to ensure compliance and to provide forensic analysis ability.

Segregation of Duties

In addition to mandatory employee background checks at all levels of Dataflow Group operations, job responsibilities are segregated. The Principle of Least Privilege (PoLP) is followed and employees are given only those privileges that are necessary to do their duties.

Physical Access

All Dataflow Group facilities and third party managed data center maintain stringent physical security policies and controls. The first layer of security includes a biometric authentication and Photo ID Badges which are to be displayed by employees at all times.

Guarded Premises

On-premise security guards monitor all alarms, personnel activities, access points, shipping and receiving, and ensure that entry and exit procedures are correctly followed on a 24/7 basis. Guards are provided with ongoing awareness training and skill-building. Numerous CCTV video surveillance cameras are located at all entry and exit points and other secured areas within the perimeter. Video is monitored and stored for review for non-repudiation.

Incident Management

Dataflow Group has defined a robust incident management process for security related events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the information security team logs and prioritizes it according to its severity. Highest priority is assigned to events that directly impact customers. This process defines courses of action, procedures for notification, escalation, mitigation, and documentation. If an incident involves customer data, Dataflow Group will promptly notify the customer of the incident and take reasonable steps to mitigate its adverse effects.

Best-In-Class Security Team

Dataflow Group employs a best-in-class global security team led by our Head of Information Security who comes with a Masters in Management of Information Systems from The London School of Economics, UK and has worked for Big 4 accounting firms including EY, KPMG and Deloitte leading various engagements in their Enterprise and Cyber Risk Advisory Services verticals and ensuring the clients compliances to the regulatory, SOC 1, 2 and specific ITGC requirements.

The Information Security team is responsible for defining / implementing policies, procedures and controls with respect to the security requirements for the sensitive client data / Personally identifiable information (PII), maintaining compliances in purview of SOC 2 compliance program, BCP/DR planning and management. All access to production is reviewed by the security team on a periodic basis.

Grievance and Data Management

In order to protect our data subjects from misuse of data and to ensure that data is maintained up-to-date, we provide access to our data protection office and grievance officer via email at speakup@dataflowgroup.com. Applicants and clients may address The Data Protection Officer on this email address, and can expect to receive a response within 48 hours of submission.

DATAFLOW

Performance Audits

DataFlow Group Operations management implements such auditing controls as appropriate for ISAE 3000 (SOC 2) Type II and ISO/IEC 27001 compliance. DataFlow Group has adopted a comprehensive eight (8) stage approach to risk management process to identify the risks within the organization based on ISO 27000 series of standards. Periodic audits are carried out to help ensure that personnel performance, procedural compliance, equipment serviceability, updated authorization records and key inventory rounds are above par.

Security Certifications

DataFlow is SOC 2, Type 1 certified and manages data in line with three trust principles - security, availability and confidentiality. It expects to achieve SOC 2 Type 2 compliancy by Q2 2018. DataFlow Group has defined its Information Security Management System in accordance with ISO 27000 series standards.

DataFlow Group's ISAE 3000 Type I audit is prepared by and audited by a Big Four accounting firm. ISAE 3000 Type I reports show that we have been through an in-depth audit of our control environment, including controls over data and network security, backup and restoration procedures, system availability and application development.

Availability

Service Level Commitment

DataFlow Group's Service Level Commitment (SLC) guarantees a 99.9% uptime (outside the scheduled service windows) for the VeriFlow production applications for all our customers. We have consistently averaged an actual uptime of 99.98%.

Data Hosting

The DataFlow group has traditionally held data within its own fileserver equipment housed in its own data centres.

Where these data centres are being used, we ensure that all systems are operating with adequate levels of redundancy, clean redundant power sources, and fire suppression systems capable of managing a fire related incident without data loss (i.e. dry protection systems).

However, as a strategic move, The DataFlow Group are making more and more use of hosted data services from large-scale global 'cloud' services such as Amazon and Google. We are actively following a migration plan which will see all Data Subject data being hosted on these cloud-based services over time.

Data Privacy

DataFlow understands the rights of both the applicant and the client, and we remain conscious and sympathetic to the needs of various data protection acts in the jurisdictions in which we operate.

We model a number of our key policies and data protection principles on the UK Data Protection Act, 1998, and as such we know applicants have rights to see the data which we hold related to them, facilitate the need to keep that data up-to-date. DataFlow is proactively addressing compliance with the General Data Protection Regulation (GDPR), due for general release in May 2018.

Use of Cookies

A cookie is a small file of letters and numbers that we store on our applicants' browser or the hard drive of our applicants' computer. We use session cookies, which are stored on our applicants' hard disk for the duration of the link, to deliver, measure and improve their experience on our website. Session cookies are automatically deleted as soon as our applicants' leave our website or the dialog is ended.

We also use Google Analytics to collect information about our applicants' online activity on the website, such as the web pages they visit, the links they click, and the searches they conduct on the website. We use the information to compile reports and to help us improve the website. The cookies collect information in an anonymous form, including the number of visitors to the website and the pages they visited. For more information about the information gathered using Google Analytics please visit

http://www.google.com/intl/en/analytics/privacyoverview.html

Processing

We only collect personal data that is actually needed to undertake the work at hand and to process the case, and we ensure that we collect that data by lawful and fair means. We process personal data fairly and only for those purposes we have agreed with applicants, with their consent and for purposes permitted by them or as permitted by applicable law. In addition, we are open to any objections from our applicants to certain types of processing as expressly permitted by applicable law.

DataFlow goes to extreme lengths to verify data from applicants, and as such makes every attempt it can to source verification from the primary source - even if this means physical visits in some cases. Under these scenarios, DataFlow may make use of country specialists, and hence we may share some of the personal data we hold with those specialist in order for us to attain the PSV. But again, we only share the information which is required to undertake the verification.

Retention

In compliance with many global data protection regulations and applicable laws, DataFlow will keep our applicants' personal data for a period of eight (8) years post which it shall be either deleted or made anonymous.

Rights

We provide our applicants with the ability to obtain a copy of their data, and the ability to ensure that data maintained on an applicant is up to date and accurate. Most data can be updated by the individual through our on-line systems, but where this is not the case, requests for adjustment may be made by contacting the Data Security Office on speakup@dataflowgroup.com. The Data Security Office may also be contacted in order to obtain a complete, portable set of data.

Security and Confidentiality

We treat personal data in a confidential manner and limit access to the data to only those who specifically need it to undertake the processing activity. We refer to industry standards and use reasonable administrative, technical and physical security measures to protect our applicants' personal data from unauthorised access, destruction, use, modification or disclosure.

In some cases the data may be shared with third parties where it enables us to undertake the verification required.

Data Sharing

We only share personal data with third parties where it is necessary to provide them with products or services or as part of the nature of our relationship with them, where we have previously informed or been authorized by them, in connection with our efforts to reduce fraud or criminal activity, or as permitted by law.

Responsibility

Each employee within DataFlow Group may only process our applicants personal data in accordance with these Principles. We conduct training and reviews of our compliance with these Principles. Employees who violate these Principles may be subject to disciplinary action, up to and including dismissal.

Accountability

Our applicants may enforce these Principles in their country against any company in the DataFlow Group that is responsible for their personal data, as a third party contractual beneficiary to these Principles. If our applicants have a complaint that we have breached these Principles and have attempted in good faith to resolve the complaint through our customer service process, but the complaint was not resolved by us within a reasonable amount of time, then our applicants may enforce these Principles against us. If our applicants complain to their local data protection authority and the data protection authority finds that we have breached these Principles, we will abide by the findings of the data protection authority, but we reserve the right to challenge or appeal such findings. These Principles do not affect any rights our applicants have under applicable law, the requirements of any applicable regulatory data protection authority, or any other type of agreement that our applicants may have with us.

DATAFLOW

Appendix 1 - List of Personally Identifiable Information Fields

The DataFlow Group has classified the following fields as Personally Identifiable Information.

- Scanned Documents
- Full Name
- Passport Number
- Email Address
- Physical Address
- Telephone Number
- Pearson VUE Registration ID
- Staff Number / Employee Code
- Seat / Roll / Hall Ticket Number
- Registration / Enrolment / License Number
- Bank Account / Receipt Number

DATAFLOW

www.dataflowgroup.com