INCLARITY

COMPLIANT

inclarity

01

INTRODUCTION

Data security is such a big issue today that it often tops the headlines in both global and national news media.

This emphasises how important it is that every business understands its compliance obligations, and how best to address those obligations.

For technology service providers and resellers, there is a potential opportunity here to help the customer understand the challenges, and the associated risks.

In a landscape where it is becoming increasingly important to differentiate, customers will trust and remain loyal to the organisations that offer them useful advice in key compliance areas.

In this document we try to explain a number of compliance issues in simple terms, and detail how Inclarity can help.

For questions about this document, or for more information not found in this document, please contact Jaci Hale by emailing **jaci.hale@inclarity.co.uk** or calling **0207 987 8080**.

02

PCI DSS COMPLIANCE

The Payment Card Industry Data Security Standard (PCI DSS) is devised and moderated by the PCI Security Standards Council, a global forum that was created some time ago specifically to offer guidance to the payment card industry on matters of data security.

The latest version of the PCI DSS standard is V3.2.1 which was released in May 2018, and which supersedes all previous versions. It can be downloaded from the Council web site here:

https://www.pcisecuritystandards.org/document_library

This standard itself is not statutory, but affects the way that your organisation can conduct business.

If you are an organisation that takes any payment from customers by card, then your payment processor will ask you to confirm whether or not you are compliant with the PCI DSS standard. Taking payments remotely without the card holder physically present presents an element of risk and compliance means demonstrating that you have understood and considered that risk.

If you are a small business you can self-certify your compliance following a relatively simple process, but if you are a large enterprise you will likely need to be audited by an accredited PCI DSS professional.

If you report to your payment processor that you are non-compliant you will receive a surcharge as a penalty on your bill from them. The size of the penalty will reflect the degree of risk this represents – factoring in the size of your business, and the number of transactions you conduct on a regular basis.

In fact, some banks now refuse to do business entirely with organisations who declare that they are non-compliant with the PCI DSS standard. Even where the payment processor may initially take a softer view, they are likely to revoke your ability to take payments entirely in the face of long-term non-compliance, or in the event of a data security breach.

Subscribing to the PCS DSS standard is therefore a good way of ensuring that you are following data protection best practice, protecting your customers and assuring your relationship with your bank and payment provider.

Key elements of the standard include:

- Checking the backgrounds of all employees who may have access to customer payment data.
- Ensuring that employees are not able to copy or save payment data that is shared with them.
- Ensuring that any payment data retained by your organisation for recurring payments – whether in physical or digital format – is properly secured from public or illicit access.
- Ensuring that any payment data sent to your organisation is transmitted in a manner which is properly secure and protected from tampering or eavesdropping.

It follows that if a customer gives you their card information over the phone for a one-time payment:

a) You must not keep the card information for longer than is needed to process the transaction.

b) You must not save or write down the card information anywhere – even temporarily – in a manner which could be viewed or accessed by any other person who is not the card holder.

c) The portion of the phone call where the card details are spoken must not be recorded.

d) Where a VoIP telephone is used to receive the call, the local network side of the phone call must be protected from tampering or snooping.

02

2.1

INCLARITY CALL RECORDING SUPRESSION

If your organisation is using Inclarity for both voice calls and voice call recording, Inclarity can offer a tool which allows you to pause the call recording when payment card details are being discussed.

This pause can be manually triggered by the VoIP user by pressing a button on their phone or on their screen, or the pause can be automatically triggered by opening a particular URL in your browser that the tool can recognise as criteria for stopping the recording.

The automatic method is recommended as it offers a higher level of compliance. If your organisation chooses to adopt the manual method, then this comes with the risk of your employees forgetting to press the button to pause the recording – and if you do not have a method of identifying these errors then you are not fully compliant with the standard.

2.2

INCLARITY COMPLIANCE CAVEAT

It is important to note that while an automated suppression tool will take your call recordings out of scope this does not automatically guarantee your compliance to the PCI DSS standard, as you may still need to address the other ways that your organisation needs to be compliant.

In fact, even if you do not record your calls, using VoIP presents some specific compliance challenges. In particular, you will need to take steps to ensure that your VoIP phones cannot be accessed illicitly via your local network – appropriate measures include:

- Putting your handsets on different, segregated network infrastructure to your PCs.
- Protect network ports reserved for the telephone network from being used by other non-telephone devices.
- Deny access from non-phone devices to the VoIP phones on your network

It follows that using IP handsets on a segregated network is significantly more compliant than using soft phones on PCs in a manner which cannot be segregated.

To gain a greater understanding of the PCI DSS standard and your level of compliance, you should seek the advice of an accredited PCI DSS professional.

03

GDPR COMPLIANCE

The General Data Protection Regulation (GDPR) is new European legislation regarding the processing of Personal Data which came into effect in May 2018.

If you are an organisation which processes any Personal Data for any reason then you will have already been obligated to take steps to ensure your compliance to the new legislation.

Some important parts of the compliance process include:

- Ensuring that the Personal Data that you retain – in printed or electronic form – is appropriately secured and protected from public or illicit access.

- Ensuring that you have an appropriate justification for retaining Personal Data, and that your Data Subjects are notified of these reasons and (where appropriate) are given the opportunity to opt into your data collection process only for those reasons.

- Ensuring that if you share the Personal Data you have collected with any third party Sub-Processors that a) the Data Subjects are made aware of this and b) you seek appropriate commitments of compliance from these third party Sub-Processors.

- Ensuring that you and any Sub-Processors do not keep Personal Data longer than it is needed.

- Ensuring that Data Subjects can request to see the data you hold on them, and where an opt-in was originally offered, provide the opportunity at any time after the fact for them to opt out.

- The Personal Data that you collect must only be transmitted or kept in a country within the EU, or which has a data sharing agreement with the EU.

The GDPR standard has some similarities to PCI DSS compliance regarding the security of data, except that treatment of Personal Data has much wider consequences. Also it is important to note that while adherence to PCI DSS is only recommended, adherence to GDPR is a mandatory legal requirement.

In the UK this GDPR legislation is being enforced by the Information Commissioner's Office (ICO), which has the right to issue fines of up to €20million, or up to 4% of annual global turnover, whichever is higher. Their guidance on the legislation can be found here:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

In the event that your organisation suffers a data breach, it must be immediately reported to both the ICO and the affected Data Subjects. In the event that is it determined that the breach was caused by non-compliance then the highest penalties will be applied. Any affected Data Subjects also have the legal right to claim compensation from the breached organisation.

Most organisations appoint a Data Controller to investigate and manage matters pertaining to data protection compliance, and for some types of organisations, this appointment is mandatory.

Note however that the text of the legislation makes it clear that any liability for non-compliance falls to the owners of the organisation, and employees cannot be individually held responsible or culpable for non-compliance.

3.1

DEFINITION OF PERSONAL DATA

The ICO's guidance indicates that:

> **"Personal data is information that relates to an identified or identifiable individual."**

In practice this means that if you have gathered sufficient information to name an individual and have the means to contact them, know their location, and/or profile their behaviour in a manner that distinguishes them from other individuals then this information is Personal Data.

It does not matter whether the information is gathered in a business-to-consumer context or a business-to-business context: any personally identifiable information is considered Personal Data.

For example, if you keep a roster of supplier or vendor contacts for the reference of your organisation, and those contacts include individual names, postal addresses, email addresses and/or telephone numbers, then this information must be treated as Personal Data.

Note however information that is not personally identifiable is not Personal Data:

- A main telephone number that can be answered by many different unidentified people
- A generic email address (such as sales@company.com) that sends messages to be read by multiple unidentified people
- A business postal address supplied without the individual, identifiable names of any people who work there

Personal Data may be gathered by an organisation in many contexts. In addition to interacting with customers, partners and suppliers, it is important to remember that when an organisation employs individuals, this means that the organisation will need to process the Personal Data of these employees.

If there is any doubt regarding the status of any data that your organisation holds, then it is best to consider that data to be Personal Data.

3.2

JUSTIFICATIONS FOR RETAINING PERSONAL DATA

All organisations must have a lawful basis for processing Personal Data.

- The processing is necessary for the performance of a contract to which the Data Subject is party to, or to take steps in advance at the request of an Data Subject which will be entering into a contract.

- The processing is necessary for compliance with a legal obligation to which the Data Controller is subject – e.g. data retention under the Investigatory Powers Act 2016 or call recording to satisfy MIFID II (see below).

- The processing is necessary in order to protect the vital interests of the Data Subject, or another natural person.

- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the data controller.

- The processing is necessary for the legitimate interests of the data controller or another third party, except where these interests are overridden by the fundamental rights and freedoms of the Data Subject which require protection (in particular where the Data Subject is a child).

- The data controller has obtained the consent of the Data Subject to the processing of their Personal Data for specific, stated purposes – e.g. to order goods or sign up to a specific service.

Note that relying on the consent of the Data Subject alone when there is no other appropriate justification is a very weak position, which the Data Controller can expect to be challenged on.

It follows that even with a lawful justification an organisation must not hold more Personal Data than it needs to, and it must not hold Personal Data longer than it needs to.

3.3

INCLARITY AND GDPR

Inclarity sets out our approach to data protection in the Privacy Statement published in our web site on the link below.

https://www.inclarity.co.uk/company/privacy-policy/

We state what data we process, and our lawful justifications for doing so. We also name our Sub-Processors and provide guidance on how to contact us with any queries or data protection requests.

This statement is similar to many service providers in that Inclarity will need to collate data on resellers and customers to provide them with telephone services. When an organisation signs a contract with Inclarity, they also implicitly provide consent for Inclarity to process their Personal Data for the purpose of providing these services.

Beyond the information provided in the Privacy Statement, to facilitate our compliance Inclarity also commits to a number of best practice internal business policies regarding:

- Physical data security and access
- Electronic data security and access
- Employee background checks, training and conduct

In the sections below we will discuss the use of some specific Inclarity services and features, and the implications this use has for data protection compliance.

3.4

SMT PORTAL - MODERATE COMPLIANCE

When setting up new telephone services in the SMT portal, it is necessary to provide a name for every Subscriber Extension. It is not strictly necessary to provide a real name of an individual for each Extension, but when doing so this data becomes Personal Data. Any email address supplied for password recovery and/or voicemail forwarding purposes - if associated with an individual - would also be treated as Personal Data.

This Subscriber information can be entered by Inclarity as part of our pre-staging policy, or the information can be entered by any reseller or customer administrator user directly into the SMT portal using their own login access. Regardless of who performs this activity, it is implicit that if the information is volunteered to be entered into the portal then the individual to which the Extension pertains has provided their consent.

In the event that any individual does not wish their Personal Data to be stored in the SMT portal, then their Extension can be edited to hold generic information instead. Similarly if an individual should leave an organisation that has Inclarity VoIP services, then the defunct Subscriber Extensions should be immediately renamed or deleted. While Inclarity can facilitate these changes upon request, the onus falls upon the contracted Customer's organisation to make the request, or perform the changes themselves using their own dedicated login access.

It also follows that any party with login access to the SMT portal will at any time be able to review the Subscriber Extension data pertaining to all individuals associated with the organisation's telephone service – this includes:

- The contracted Customer
- The owning Channel reseller (if any)
- The owning Partner reseller (if any)
- Inclarity's own personnel

By volunteering any Subscriber information to be entered into the SMT portal, the Customer should be aware – and must accept - that the data is accessible to these parties in this way.

Inclarity does not vouchsafe the ongoing accuracy of any Subscriber data entered into SMT – this responsibility tacitly falls to the Customer organisation taking the service (or their managing reseller), who can manage the information on a day-to-day basis from their own portal login. Inclarity takes no responsibility for Extensions that hold legacy data, and which are not updated by the Customer in this way.

3.5

REDBOX CALL RECORDING - LOW COMPLIANCE

The Redbox Call Recording service offered by Inclarity is a legacy service which Inclarity does not vouchsafe as fully GDPR compliant. Customers continue to use the service at their own discretion and risk.

When an Inclarity Customer orders the Redbox Call Recording service, they are also normally given a Supervisor login to the Redbox portal for the purposes of reviewing historic call recordings. The nominated Supervisor will by default be offered the recordings for all of the individuals within the Customer's organisation who are currently being recorded. It is possible to compartmentalise a Supervisor's access to recordings upon request.

While the Supervisor search tool includes a number of possible search filters, the Redbox platform does not provide any capability to search the spoken content of the recorded calls. The content of a call can only be determined by playing the recorded media (or by the associated Subscriber making some external note regarding the call at the time that it occurs). Hence it is possible that the Customer many unknowingly hold Personal Data as recorded voice content which contravenes their own Privacy Policy.

A Redbox Supervisor is also given permission to download calls, with an option to take bulk archives of large volumes of calls at once. Each downloaded file is unencrypted and can be immediately played back in any audio app or desktop program. Download activity history is not recorded by the Redbox platform, meaning that the Customer's organisation will have no awareness of what has been downloaded by who and when for auditing purposes.

Note that downloaded call recordings present a significant compliance risk – if they are not downloaded to an appropriately secure file repository then they could be copied by other individuals inside or outside of the Customer's organisation. The movements of these downloaded files may also be difficult to track from a data retention perspective.

On the Redbox platform itself, the data retention period for all recorded calls is fixed to 12 months. Redbox Supervisors are not given permission to delete calls themselves either individually or in bulk. In fact Inclarity as the service provider is not able to selectively delete calls, and can only delete all calls that exceed the retention period. All Customers should bear this in mind when formulating their own data retention policies.

The Redbox platform is not fully multi-tenanted, but a single higher tier of Administrator access is available to Inclarity employees only to manage the platform on an ongoing basis. This Administrator access does provide permission to search, play back and download Customer call recordings. In a similar manner to Supervisors, the platform does not provide any activity history by Administrators for auditing purposes.

As mentioned in the earlier section on PCI DSS compliance, Inclarity does offer a suppression tool to pause the always-on recording service for a Subscriber on a manual or automated basis.

3.6

DUBBER CALL RECORDING - HIGH COMPLIANCE

The Dubber Call Recording service offered by Inclarity is a newer service which is vouchsafed by Inclarity as highly GDPR compliant.

When an Inclarity Customer orders the Dubber Call Recording service, each individual Extension user is offered login access to the Dubber portal to review, search and play back their own personal call recordings. They can also 'tag' their recordings as they happen, or after the fact, with any text string to make them easier to identify and search in the future. They can also temporarily share single recordings to third parties by sending an email containing a secure URL. These Extension users - and the people they may share their recordings to - do not have permission to delete or download their recordings.

One of more end users can be elevated to Administrator access in the Dubber portal, which provides all of the above features, but also elevates their permission to review all of the call recordings made by the same Customer's organisation, and to delete or download any of these recordings. Downloads are restricted to one call at a time (to avoid the compliance issues caused by bulk downloading), and all download activity is recorded and auditable (by the provider Dubber themselves upon request).

A higher tier of Administrator access in the same portal allows Inclarity to gain an overview of all Customers on the Dubber platform. Importantly, although this level of access allows an Inclarity employee to search for call records, this level of access does not permit that Inclarity user to play back or download the call recording, protecting the privacy of the Customer.

While the search tool offered to end users and Administrators includes a number of possible search filters – including self-assigned text tags - the Dubber platform does not currently provide any capability to search the spoken content of the recorded calls. Hence – similar to the Redbox platform - it is possible that the Customer many unknowingly hold Personal Data as recorded voice content which contravenes their own Privacy Policy. Having said this, Inclarity is in negotiations with Dubber to offer a call transcription product which would have many wider applications, not just in improving data protection compliance.

The Dubber Lite product offers a retention time of 6 months –any calls older that this period are automatically deleted. The Dubber Large product stores calls by volume, not by age – the 100,000 minutes per user is retained indefinitely until the storage limit is reached. The Dubber MIFID product guarantees that call recordings are kept for a 7 year period. In the case of either product, any of the Customer's Administrators can choose to delete unwanted call recordings at an earlier point in time.

As mentioned in the earlier section on PCI DSS compliance, Inclarity does offer a suppression tool to pause the always-on recording service for a Subscriber on a manual or automated basis.

Dubber is a fully hosted solution, with all data stored within Amazon Web Services UK1 in central London, presenting no compliance issues in this respect.

3.7

CALL RECORDING - OTHER CONSIDERATIONS

Where an Inclarity Customer orders either Call Recording service (Redbox or Dubber) for any Subscriber, the service remains on for all calls and regardless of content. This has implications for the Customer's organisation and their own data protection compliance in respect to their own employees – each employee should be clearly instructed not to use their business phone for personal calls where Personal Data not relevant to the organisation's normal business could be captured. Alternatively, it could be made part of the employee's contract that they acknowledge that their calls are recorded, and that they give their consent for the content of the calls they make on their business phone to be kept by the organisation.

Depending on the Customer's reasons for recording their calls, they may have a legal requirement to inform the external callers that they are being recorded, along with the reasons why they are being recorded. For inbound calls from external callers, Inclarity can provide Auto Attendant or Call Queuing features that allow the Customer to play a pre-recorded message to the caller before the call is answered. Inclarity however does not provide any means to play a recorded message on an outbound call to the caller when they first pick up the call – instead the calling party would need to announce the policy message themselves before taking the call any further.

Phone

Sales: 0800 987 80 80

Customer services: 0800 987 8000

Email

info@inclarity.co.uk

Inclarity Communications Ltd

96 – 98 King Street

Hammersmith

London

W6 0QW

Web

www.inclarity.co.uk