DRURY HOLIDAYS
DATA SECURITY POLICY

Introduction

The Financial Conduct Authority (FCA) expects businesses to conduct their business within the rules and Principles for Business they have put in place. There are 11 Principles in total; however Principles 2 and 3 are most relevant to Data Security:

2. Skill, Care & Diligence:'A Firm must conduct its business with due skill, care and diligence'.

3. Management & Control:'A Firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'.

The Data Protection Act 1998 requires every data controller (eg organisation, sole trader) who is processing personal information to register with the ICO (Information Commissioners Office), unless they are exempt.

Purpose

Drury Holidays are registered with the ICO accordingly.

During the course of daily transactions Drury Holidays collect, process and hold a variety of data relating to staff, customers, suppliers and third parties. In addition to the general need to keep personal information and commercially sensitive data confidential.

The Data Protection Act (1998)

The Data Protection Act (DPA) governs the **processing**(i.e. obtaining, holding, organising, recording, retrieval, use, disclosure, transmission, combination and destruction) **of personal and sensitive data** (i.e. data relating to a living individual - the data subject)and sets out the rights of individuals whose data is processed in manual or electronic form or held in a structured filing system. The cornerstones of the DPA are eight Principles that describe the legal obligations of firms that handle personal information about individuals. These Principles are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the DPA.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area ("EEA") unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Drury Holidays fully support these principles.

The Privacy and Electronic Communications Regulations

Within the Privacy and Electronic Communications Regulations (PECR), the marketing rules apply to communication by electronic means such as by telephone, fax, email, text message and picture (including video) message and by using an automated calling system. There are also rules relating to cookies that are set on computers when individuals browse websites and their relevance to Drury Holidays is explained separately in this document.

The FCA's Principles for Businesses

In line with FCA Principles for Businesses 2 and 3, firms must make an appropriate assessment of the financial crime risks associated with customer data and take steps to prevent the loss or theft or miss-use of such data.

The DPA and PECR are wide in their scope and have far reaching implications for Drury Holidays as we acquire, process and hold personal data about individuals. The purpose of this Data Protection policy is to summarise the regulatory requirements and senior management responsibilities to fulfil Drury Holidays's commitment to protecting and respecting the privacy of individuals whose data is processed.

Responsibilities

Drury Holidays comply with the Data Protection Act (1998) and the Privacy and Electronic Communications Regulations. In addition, the FCA's Principles for Businesses set out fundamental obligations for regulated firms, which include the requirement to treat customers fairly and maintain effective data security controls.
We understand failure to comply with any of all these regulations can lead to financial penalties, compensation payments and reputation damage for Drury Holidays.

Application

This policy applies to Drury Holidays dealings with customers and third parties that may be involved in processing customer related data. It covers the manner in which personal data should be obtained, used, shared, physically stored and destroyed. Relevant data protection related definitions have been included at the back of this document.
The obligations under the DPA also apply to our agents that introduce prospects and customers to Drury Holidays businesses.
Oversight responsibility for data protection matters will be apportioned to our nominated Data Protection Officer (Michael Drury)

Registration with the ICO

The Information Commissioner's Office (ICO) is responsible for monitoring and supervising compliance with the DPA and the PECR. Data controllers and data processors are required to notify the ICO about the type of personal information they process. Failure to register these details with the ICO is a criminal offence. The ICO has a two-tiered fee structure based on business size and turnover and registration has to be renewed annually.

Handling personal data fairly and lawfully

The first and second Data Protection Principles require businesses to acquire and process personal data fairly and lawfully for specific purposes. It is therefore necessary that Drury Holidays are clear at outset about the purpose for which data is to be obtained and processed and to be demonstrating that actions taken are fair and lawful. Michael Drury is responsible for ensuring that:
1. there are comprehensive marketing plans and operational procedures in place for initiating contact with prospects and generating sales in a manner that complies with the DPA, the PECR and the FCA's rules and guidance;
2. personal data is collected and used only when there are legitimate business reasons which are balanced against the interests of the individual concerned;
3. personal data is not used in ways that would have adverse effects on individuals;
4. the purpose or purposes for which the data is to be used is made known to individuals and they are given appropriate privacy notices when data is collected;
5. personal data will only be handled in ways that individuals would reasonably expect; and
6. the data will be used fairly and lawfully.
7. at request, disclose to the customer where their data was obtained
8. take reasonable steps not to pass data for a regulated product to a non-regulated company Drury Holidays will not make unsolicited calls to numbers entered on the PECR register under regulation 25 or 26 or to a client who has notified us not to be called.
These steps will be taken across all customer contact and distribution channels, e.g. business conducted via agents, Drury Holidays call centres and through corporate websites. Adequate records will be maintained to demonstrate compliance with the above-mentioned requirements. A privacy notice may be used as a separate document where the above points cannot be easily integrated into the sales process.
Where telephone calls with customers are recorded for monitoring and/or quality assurance or training purposes this is disclosed to customers at the start of each call. In this regards Michael Drury ensures that:
a) suitable telephone scripts for in-bound and out-bound calls are available to staff; and
b) the scripts clearly contain the requirement to disclose to customers that the call is being recorded for monitoring or quality assurance or training purposes.

Consent

When conducting business, customer data is usually collected using a hardcopy or an online application form. Consent to collect and process personal data can be obtained by inclusion of appropriate wording on the form in an efficient and fair manner. If contact is by telephone only the use of scripts designed to seek consent. The key is careful consideration of the marketing activities that are to be carried out with the captured data and inclusion of appropriate, informative wording and consent options so that the prospect or customer is made fully aware of the manner in which their personal data will be used by the company.

The European Data Protection Directive (to which the DPA gives effect) defines an individual's consent as "…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". It is necessary to examine the circumstances to decide whether consent has been given, as it may not always be obvious. Consent must be:

Informed: the individual must be provided with sufficient information to make a decision as to whether or not he wishes the processing to go ahead;

Specific: in respect of specific data processing activities, such as to offer regulated products;

Signified by the individual unambiguously: the individual must take positive action to show consent and silence will not suffice;

Given freely: consent is not obtained under duress or where the individual is given no real opportunity to say "no".

When an individual "opts-in" they actively consent to receiving direct marketing material by ticking the consent box, whereas under the "opt-out" option the individual objects or does not take up the opportunity to receive the material.

Even when consent has been given, it will not necessarily last forever. The individual may withdraw consent, depending on the nature of the consent given and the circumstances in which the data was collected or used. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

Under the PECR there are specific requirements relating to unsolicited direct marketing communications. A solicited communication is one that is actively invited, either directly by the customer or via a third party. An unsolicited communication is one that the customer has not invited but they have indicated that they do not, for the time being, object to receiving it. If challenged, businesses would need to demonstrate that an individual has positively opted in to receiving further information from the business.

Drury Holidays understand that it is unlawful to contact customers or organisations that have informed or managed preference service providers that they do not wish to receive unsolicited marketing material. Therefore, Drury Holidays are aware of and comply with the following:

Telesales – Drury Holidays ensure that individuals and organisations they wish to contact are not registered on the Telephone Preference Service (TPS) or the Corporate Telephone Preference Service (CTPS) respectively. If they are registered or have directly notified Drury Holidays not to call, then unsolicited direct marketing calls will not be made to them.

Faxes – similarly individuals and organisations that have registered with the Fax Preference Service ("FPS") or have directly notified Drury Holidays not to contact them by fax, will not be sent unsolicited direct marketing faxes. Emails and text message – Drury Holidays will not contact individuals by email or via text message without obtaining prior consent unless the individual's details have been obtained in the course of a sale or negotiations of a sale. Furthermore, email a nd text contact will only be about similar products or services offered by Drury Holidays. Individuals will be given the opportunity to opt out of receiving further marketing emails or texts each time that such contact is made. Individuals can register with the Email Preference Service (eMPS) to restrict the number of direct marketing emails they receive and therefore a cross-check with the eMPS database is conducted before launching any email marketing campaigns.

Requirements relating to marketing by post fall under the DPA. The Mailing Preference Service (MPS) is managed by the Direct Marketing Association and supported by Royal Mail so as to enable individuals to register their names and addresses to limit the amount of direct mail they receive. Unsolicited marketing material will not be sent by post to individuals that have informed Drury Holidays they do not wish to receive such information or they have registered with the MPS.

Drury Holidays maintain internal logs of individuals and organisations that have indicated that they do not wish to receive unsolicited marketing information and also conduct checks against the TPS, CTPS, FPS, eMPS and MPS databases as appropriate to suppress contact with individuals listed on internal logs and preference service registers.

Michael Drury is responsible for ensuring that:

1. every prospect's and customer's consent has been obtained in advance before any email and text based marketing is initiated, if their personal details were not obtained in the course of a sale or during sales negotiations;
2. consent is absolutely clear (which, in the case of sensitive personal data has to be explicit consent);
3. consent received covers specific purposes and type of processing that the company wishes to carry out including any disclosures of personal information that may be made to third parties or intention to transmit data overseas;
4. customers are made aware of how they can opt out of receiving further marketing information at any time; and

5. consent has not been withdrawn through direct notification to the company or via registration with the TPS or FPS or eMPS or MPS (and in the case of organisations, via the CTPS) before unsolicited marketing information is sent to customers.
If data is purchased from third parties for prospecting purposes, Drury Holidays ensure that the data has been acquired by the third party through fair and lawful means, the data can be used for the purposes of unsolicited marketing activities and that the data has been cross-checked by the third party against the appropriate preference service databases.
According to the ICO, a particular consent may not be adequate to satisfy the legal condition for processing (especially if customers might have had no real choice about giving it). For these reasons the ICO recommends that businesses will not rely exclusively on consent to legitimise processing but instead concentrate on making sure that individuals are treated fairly.

PECR and cookies

Under the PECR as from 26 May 2011, businesses must seek consent before any cookie is set on an individual's computer. Cookies are small, often encrypted text files, located in browser directories. They are used by companies to help users navigate websites efficiently and perform certain functions. Cookies are also used to keep computer users logged in and their personal details private or for tracking their activity so that companies can improve the website.
Cookies can be used by third parties to track information about individuals and spam them with adverts. By themselves, cookies pose no risk since they do not contain viruses.
Session cookies enable the website to track user movement from page to page so that the user does not get asked for the same information again. The most common example of this functionality is the shopping cart feature of an ecommerce website. Session cookies are never written on the hard drive and they do not collect any information from the user's computer. Session cookies expire at the end of the user's browser session.
Persistent cookies are stored on the user's computer and are not deleted when the browser is closed. Such cookies can retain user identities and preferences, allowing those preferences to be used in future browsing sessions.
Michael Drury is responsible for ensuring that Drury Holidays websites comply with the PECR and that, where necessary, appropriate information is disclosed to website users and consent is obtained from users before cookies are set.

Fair treatment

Fairness generally requires the company to be transparent, i.e. clear at outset and open with individuals about why the information is being collected and how it will be used. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair. The DPA states that information will be treated as being obtained fairly if it is provided by a person who is legally authorised, or required, to provide it.
The law gives companies some discretion in how they provide fair processing information – ranging from actively communicating it to making it readily available. The oral or written statement that individuals are given when information about them is collected is often called a "fair processing notice" or "privacy notice". Companies often adopt phrases such as "how we use your information" to explain the purpose of collecting and processing information''.
Taking this into account, Drury Holidays ensure that, in all cases, consent and privacy statements will:
be clear, fair and not misleading;
explain the consequences of not providing the required information;
explain how long the information will be kept for;
explain if the replies to questions are mandatory or voluntary;
explain if the information will be transferred overseas;
explain that if the information will be shared, who with and how they will use it;
explain how customers may be contacted e.g. telephone, email, SMS, post;
explain customers' rights – e.g. they can obtain a copy of their personal information;
explain who to contact if they wish to know more information about how their information is held or to opt-out of receiving further information or if they need to complain; and
explain customers' right to complain to the Information Commissioner.
Michael Drury is responsible for ensuring that the following details are communicated to customers:
1. the identity of the business or if appropriate, its nominated representative;
2. the purpose(s) for which the business intends to process the prospect's or customer's personal information and if the information is to be shared or disclosed to other organisations (so that the individual concerned can choose whether or not to enter into a relationship with the company sharing it);
3. any additional information that will enable the business to process the information fairly; and
4. how customers can access the information held about them (as this may help them to spot inaccuracies or omissions in their records – see section below on Rights of Data Subjects).

Lawful processing and compatibility

The DPA requires businesses to specify the purpose or purposes for which they obtain personal data and ensure that anything they do with the data must be compatible with those purposes and is lawful. Michael Drury is responsible for ensuring that, when processing customer data, Drury Holidays does not:
commit a criminal offence by failing to comply with the lawful processing requirement;
breach the company's implied or stated duty of confidence;
exceeds its legal powers or exercises those powers improperly;
infringe copyright;
breach an enforceable contractual agreement;
breach industry specific legislation or regulations;
breach the Human Rights Act 1998, specifically the right to respect private and family life, home and correspondence.

Minimum amount of personal data

Under the third Data Protection Principle Drury Holidays identify the minimum amount of personal data we need so as to properly fulfil our purpose. We ensure that we hold that much information, but no more. If we need to hold particular information about certain individuals, we only collect the information for those individuals and no more. Drury Holidays do not hold personal data on the off-chance that it might be useful in the future.
Michael Drury ensures that only minimum amount of personal information required for normal business activities is collected and held. Checks are conducted to ensure that excessive or irrelevant information is not held as there is a risk that the information will be out-of-date.

Accurate and kept up-to-date

The DPA does not define the word "accurate", but it does say that personal data is inaccurate if it is incorrect or misleading as to any matter of fact. It will usually be obvious whether information is accurate or not. To comply with this,
Drury Holidays:
take reasonable steps to ensure the accuracy of any personal data they obtain;
ensure that the source of any personal data is clear;
carefully consider any potential challenges as to the accuracy of information; and
consider whether it is necessary to update the information, particularly if the purpose relies on the information being current.
Michael Drury ensures that:
1. staff have accurately recorded information provided by prospects and customers, or by another individual or organisation;
2. reasonable steps are taken to determine the accuracy of the information; and
3. if the individual has challenged the accuracy of the information, this is evaluated and recorded.
Drury Holidays understands that an expression of an opinion about an individual is classed as their personal data. The record of an opinion (or of the context it is held in) will contain enough information to enable a reader to interpret it correctly. If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, Drury Holidays understand that it is even more important to state the circumstances or the evidence it is based on.
If a court decides that a business is holding inaccurate personal data containing an expression of opinion that is found to be inaccurate, it can order the deletion of that data. Any remarks made in emails or system notes would need to be disclosed if the individual or the court requests personal information. Therefore, Drury Holidays ensure that emails do not contain anything that might be considered derogatory, or offensive, even though the record is generally for internal use.

Data retention

To comply with Data retention, Drury Holidays establish standard retention periods for different categories of information, keeping in mind any professional rules or regulatory requirements that apply and ensuring that those

retention periods are being applied in practice. Any personal information that is no longer required will either be archived or deleted in a secure manner.
Drury Holidays's Retention periods for different categories of personal data are based on individual business needs. A judgement is made about:
the current and future value of the information;
the costs, risks and liabilities associated with retaining the information;
the ease or difficulty of making sure the data remains accurate and up to date; and
the ease with which historic data will be accessible, should it be necessary to respond to a data subject request (see section below on Rights of Data Subjects).
Drury Holidays understand the difference between permanently deleting a record and archiving it. If a record is archived or stored offline, it will reduce its availability and the risk of misuse or mistake. If it is appropriate to delete a record from a live system, Drury Holidays will also delete the record from any back-up of the information on that system, unless there are business reasons to retain back-ups or compensating controls in place. Michael Drury is responsible for:
1. reviewing the length of time personal data is kept based on the categories (e.g. quotations, historic and new sales, lapsed contracts, etc) under which such information is collected and held;
2. considering the purpose or purposes of the information in deciding whether to retain it and for how long the information will be retained;
3. suppressing information about individuals and organisations that have indicated (to Drury Holidays or by registering with any of the preference service providers) that they do not want to receive unsolicited marketing material;
4. securely deleting information that is no longer needed for the purpose it was obtained;
5. updating, archiving or securely deleting information if it goes out of date or if the retention period has expired; and
6. ensuring that regular audits are conducted to check that personal data is not held for longer than is necessary by the business and any third parties with whom the information is shared.
Personal details relating to existing customers and policies that are in force are held in accordance with the relevant FCA requirements.

Rights of Data Subjects

The sixth Data Protection Principle relates to specific rights of individuals (i.e. Data Subjects) whose personal data is obtained and processed by businesses. Data subjects have:
a right to have access to a copy of the information comprised in their personal data;
a right to object to processing that is likely to cause or is causing damage or distress;
a right to prevent processing for direct marketing;
a right to object to decisions being taken by automated means;
a right to have inaccurate personal data rectified, blocked, erased or destroyed; and
a right to claim compensation for damages caused by a breach of the DPA.
An individual who makes a written request is entitled to be:
told whether any personal data is being processed;
given a description of the personal data, the reasons it is being processed, and whether it will be shared with any other organizations or individuals;
given a copy of the information comprising the data; and
given details of the source of the data (where this is available).
An individual can also request information about the reasoning behind any automated decisions, such as a computer generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).
Michael Drury is responsible for ensuring that Drury Holidays respond to a subject access request promptly and in any event within 40 days of receiving it, bearing in mind the following requirements:
for a subject access request to be valid, it must be made in writing (including by email and fax);
if a request is made verbally the requirement to make a request in writing is explained;
if a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, then the request may be treated as though it were valid and the response must be given in a format which is accessible to the disabled person, such as Braille, large print, email or audio formats;
if a request does not mention the DPA specifically or even say that it is a subject access request, it is nevertheless valid;
a request is valid even if the individual has not sent it directly to the person who normally deals with such requests within the business.
When Drury Holidays receive a subject access request, we can charge a fee of £10 in accordance with ICO guidance.
In line with the DPA, Drury Holidays will request certain information before responding to a request:

enough data to judge whether the person making the request is the individual to whom the personal data relates so as to avoid personal data about one individual being sent to another, accidentally or as a result of deception; information that would reasonably be required to find the personal data amongst the records held by the company and covered by the request.
In the event of an individual making a subject access request via a third party Drury Holidays will request written consent from the individual to confirm that the third party can request and receive information on the individual's behalf.

Requests for information from law enforcement agencies

The DPA includes exemptions, which allow personal data to be disclosed to law enforcement agencies without the consent of the individual who is the subject of the data, and regardless of the purpose for which the data were originally gathered. Drury Holidays will release personal data to law enforcement agencies if:
the information is required for safeguarding national security; or
failure to provide the data would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty.
Police forces have standard forms (known as section 28/section 29(3) forms) for requesting personal data, in accordance with guidance issued by the Association of Chief Police Officers ("ACPO"). The form must certify that the information is required for an investigation concerning national security, the prevention or detection of crime, or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information. If Drury Holidays receives one of the above forms, we will supply the data under the DPA exemptions.
If Drury Holidays receive data subject access requests from other law enforcement agencies such as The National Crime Agency (NCA), or HMRC, we will supply the requested data so long as the request:
be in writing, on headed paper, and signed by an officer of the agency;
describes the nature of the information which is required;
describes the nature of the investigation (e.g. citing any relevant statutory authority to obtain the information); and
certifies that the information is necessary for the investigation.

Data security

To comply with the seventh Data Protection Principle, Drury Holidays has appropriate security measures to prevent personal data held being accidentally or deliberately compromised. In particular, Drury Holidays:
have designed and organised security to fit the nature of the personal data held and the harm that may result from a security breach;
are clear about who in the business is responsible (Michael Drury) for ensuring information security;
make sure that right physical and technical security is in place, backed up by robust processes and procedures and reliable, well-trained staff; and
are ready to respond to any breach of security swiftly and effectively.
Drury Holidays recognise that data security breaches may cause real harm and distress to the individuals if their personal data is lost or abused (sometimes linked to identity fraud) which can lead to:
fake credit card transactions;
false references to acquire tenancy;
With advances in technology, businesses are equipped to process more and more personal data and to share information more easily. The more databases that are set up and the more information is exchanged, the greater the risk that the information will be lost, corrupted or misused. Drury Holidays understand this and recognise the importance of safeguarding personal data as not ensuring this may lead to financial penalties imposed by regulators in addition to payment of compensation for any losses suffered by individuals.
The Computer Misuse Act (1990) identifies three specific offences:
i. unauthorised access to computer material (that is, a program or data);
ii. unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime; and
iii. unauthorised modification of computer material.
Drury Holidays consider the following security measures as part of our risk management obligations:
Physical security, to ensure that:
access to business premises is restricted through key pad entry, door buzzers, etc;
visitor access is recorded centrally and supervised at all times; and
alarms and CCTVs are installed to protect premises and business assets during non-working hours.
Managing and monitoring staff, to ensure that:
staff are aware of, trained and comply with regulatory requirements and company policies on data protection and information security matters;
staff handling customer or confidential business data are honest and trustworthy;
staff do not disclose information about customers without checking the identity of callers and verifying that they are entitled to the data being requested;

only authorised staff can access, alter, disclose or destroy personal data;
managers and staff only act within the scope of their authority;
paper records containing customer data and commercially sensitive information is stored securely when not in use,and desks are cleared at the end of the working day; and
data destruction or disposal is adequately supervised.
Computer systems and effectiveness of controls around:
access to information captured on call recording systems;
emails for business communications;
use of laptops, blackberries and removable media e.g. USB keys, CDs etc;
requent use of spreadsheets to analyse data;
remote working arrangements; and possibility of electronic communications being intercepted or being sent to incorrect destinations.

Encryption

Encryption refers to algorithmic schemes that encode plain text into non-readable form or cypher text, to provide privacy.
The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form. The key is the trigger mechanism to the algorithm.
The internet, email and instant messaging are open in nature and without encryption. The information is not only available for anyone to read but the data could be held for years on servers that may change hands or become compromised in a number of ways. Encryption of emails can be accomplished with programs that feature plug-ins or interfaces for popular email clients or customers or suppliers Web browsers will encrypt text automatically when connected to a secure server, evidenced by an address beginning with
https. The server decrypts the text upon its arrival, but as the information travels between computers, interception of the transmission will not be fruitful to anyone as it will be unreadable.
Michael Drury is responsible for ensuring that customers' personal data and confidential information about Drury Holidays activities are not transmitted electronically in an unencrypted format. In addition where commercially sensitive data is to be shared with third parties via USB keys or CDs, these devices are also encrypted.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) was put together by the PCI Security Standards Council to decrease payment card fraud across the internet and increase credit card data security. Drury Holidays comply with the PCI-DSS requirements, this is enforced by the 'acquiring bank' through whom we have our merchant account.
There are twelve key requirements for organisations:
1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for passwords or other security parameters.
3. Protect stored data.
4. Encrypt the transmission of cardholder data and sensitive information.
5. Use and regularly update anti-virus software.
6. Develop and maintain securer systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.
There are four levels of validation requirements, based on processing volume:

Level Merchant Criteria Validation Requirements

1 Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region Annual Report on Compliance ("ROC") by Qualified
Security Assessor ("QSA") or Internal Security Assessor ("ISA") if signed by officer of the company
Quarterly network scan by Approved Scan Vendor ("ASV") Attestation of Compliance Form
2 Merchants processing 1 million to 6 million Visa transactions annually (all channels) Annual Self-Assessment Questionnaire ("SAQ") Quarterly network scan by ASV Attestation of Compliance Form
3 Merchants processing 20,000 to 1 million Visa ecommerce transactions annually Annual SAQ
Quarterly network scan by ASV Attestation of Compliance Form
4 Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually Annual SAQ recommended Quarterly network scan by ASV if applicable
Compliance validation requirements set by merchant bank Drury Holidays understand the importance of complying

with the above key requirements and four levels of validation and it is Michael Drury's responsibility to ensure that we remain compliant with the PCI-DSS.

Outsourcing

Drury Holidays have procedures in place if we use third parties to process data to ensure that we:
only choose a data processor that provides sufficient guarantees about its security measures to protect the data and the processing it will carry out;
take reasonable steps to check that those security measures are working effectively in practice; and
put in place a written contract setting out what the data processor is allowed to do with the personal data or business information.
The outsourcing contract requires the data processor to take the same security measures that we have in place, as if we were processing the data. This is because the regulator will hold us accountable if the third party fails to take adequate steps to protect our customer data. To ensure that this is adhered to, we use the European Committee for Standardisation's model data processing contract as a basis.
Drury Holidays undertake due diligence before engaging a third party to process data on behalf of ourselves, ensuring that the third party has adequate and effective data protection and data security controls.

Restrictions on transferring data to non EEA countries

There are no restrictions on sending personal data to EEA countries but the eighth Data Protection Principle restricts the transfer of data to non-EEA countries. It must be remembered that, the first DPA Principle (relating to fair and lawful processing) will in most cases require businesses to inform individuals about disclosures of their personal data to third parties overseas and the seventh Principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using third parties abroad to conduct business or process data.
Putting personal data on a website will often result in transfers to countries outside the EEA when someone overseas accesses the website. If businesses load information onto a server based in the UK so that it can be accessed through a website, they must consider the likelihood that a transfer may take place and whether that would be fair for the individuals concerned.
Drury Holidays considers the following factors when deciding whether or not to transfer data overseas:
the nature of the personal data being transferred; how the data will be used and for how long; and
the laws and practices of the country where data is being transferred to.
Drury Holidays conduct a risk assessment to ensure there is enough protection for individuals, in all the circumstances of the transfer. We also consider additional factors such as:
the extent to which the country has adopted data protection standards in its law;
whether there is a way to make sure the standards are achieved in practice; and whether there is an effective procedure for individuals to enforce their rights or get compensation if things go wrong.

Data loss

If personal data is accidentally lost, altered or destroyed, it must be recovered quickly to prevent any damage or distress to the individuals concerned. In this regard Drury Holidays consider the following:
i. containment and recovery – the response to the incident must include a recovery plan and, where necessary, procedures for damage limitation.
ii. assessing the risks – assess any risks and adverse consequences associated with the breach, as these are likely to affect how the breach has been contained.
iii. notification of breaches – informing management, regulators, law enforcement agencies and individuals (whose personal data is affected) about the security breach is an important part of managing the incident.
iv. evaluation and response – it is important that to investigate the causes of the breach, as well as, the effectiveness of controls to prevent future occurrence of similar incidents. Clear desk guidelines
To ensure that personal or sensitive data belonging to customers and confidential business matters is not accessible or viewable by unauthorised individuals e.g. cleaners, Drury Holidays have a clear desk policy. In order to comply with this, the following is adhered to:
at the end of each working day, desks are cleared of all customer files and business documents, including any such papers held "in" and "out" trays;
photocopiers, printers and fax machines are checked at the end of each working day and any documents that have not been collected are removed and placed in a secure place;
files and documents are kept in designated storage cupboards and any papers that contain personal, sensitive data or confidential information are kept in locked cupboards or cabinets; and
at the end of each day desk top computers are always switched off and laptops are locked away if not required for remote working.

Secure disposal of records and computer equipment

Once the retention period expires or, if appropriate, the customer data or business information is no longer required;
paper records are disposed of in a secure manner. All paper records containing customer data or business information are disposed of by shredding, either on-site at the office premises or by a reputable third party that has suitable disposal arrangements in place. This includes all archived records.
Michael Drury is responsible for monitoring and maintaining internal arrangements for secure shredding and that due diligence checks are conducted before contracting with a third party to dispose of Drury Holidays records. A full audit trail is also maintained by Drury Holidays to evidence the date of destruction, the records disposed and the manner in which they were destroyed, which in the case of a third party will include certificates to confirm disposal has been carried out securely.
Drury Holidays ensure that used computers, fax machines, printers and any other equipment that may contain or that will have stored customer or corporate data in electronic format is disposed of in an appropriate manner after the information has been completely wiped off.
Drury Holidays have security controls in place to prevent the miss-use, loss or theft of customer data and business information. We also ensure that staff do not compromise the security by adequately supervising and monitoring business activities.

Monitoring & Reporting

Michael Drury is responsible for ensuring that, in the first instance, adherence to this Data Protection policy is checked and monitored.
Data protection related incidents are reported to Michael Drury and are recorded and managed as per the Regulatory Breaches & Incidents Policy. Data loss incidents are logged in addition to all Data Subject Access Requests (DSAR).

Record Keeping

Drury Holidays Ltd retain all evidence of DPA adherence.
These records are retained for 6 years.