

/MarketDeveloper

Infosecurity

A Marketer's Guide to Keeping Your Data Safe

Data is an essential part of the modern marketer's toolkit but it can be challenging to manage and protect. The security and privacy of customer data should be a top priority for any company actively storing business data.

What is PII?



PII stands for Personally Identifiable Information and protecting it is absolutely vital. PII refers to information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to

uniquely identify an individual.

In order to protect data, brands and suppliers should, at the very least, follow the simple best practice guidelines outlined below:

1) Educate and Train staff

By educating your employees and colleagues about phishing scams, security breaches, data loss and risks, as well as how to prevent the spread of viruses, you are helping to keep your organisation protected. Make everyone aware.

2) Lead by example

Never use shared computers
Only ever connect to the internet via secure connections
Passwords should be changed on a regular basis, at least every 3 months.
Passwords should be at least eight characters long and include a mixture of numbers and letters, both lower case and upper case

3) Data loss

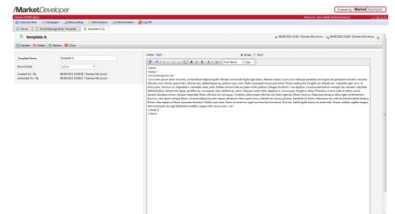
- Never hold data outside your main database on portable storage de-

vices such as portable PC's, CD's / DVD's or memory sticks

- Always encrypt, the evidence is that the majority of data is not encrypted. Cloud based systems (like MarketDeveloper) hold your data in a physically and cyber secure environment that still allows access when needed
- Never send data by email attachment
- Always use secure transfer mechanisms and use a different medium for communicating the password!

4) Keep your friends close

Make sure your supplier provides proof and guarantees with regards to the type of technical and organisational security measures it has in place. We would advocate DMA membership and ISO 9001 as a minimum, and preferably ISO27001.



5) Write a Data Security Policy.....

Having a data security strategy in place offers peace of mind to staff, stakeholders and most importantly customers. Amongst other things it means everyone should know what they need to do at any time and allows your business to react quickly and effectively to a data security incident.

.... Including a Crisis Management Plan


A carefully thought out Crisis Management Plan, or Business Continuity Plan (BCP) will help you cope

/MarketDeveloper

more easily in a potential crisis, enabling you to minimise disruption to your business and customers.

The policy should cover management commitment to information security within your organisation and clearly define who is responsible for implementing the policy. Here are a few pointers to consider when writing your BCP:

- 1) Identify your crises
- 2) Prioritise the risks
- 3) Assess the impact of a security breach
- 4) Determine how you can minimise risk
- 5) Set out a plan of how to react
- 6) Write a realistic timeline
- 7) Identify the roles of individuals within your organisation in an emergency
- 8) Ensure you have emergency contact information for all staff, particularly if a breach occurs outside office hours.
- 9) Appoint a single company spokesperson to handle PR and journalist enquiries
- 10) Ensure staff and customers are informed before they find out anything in the press



The period immediately after a security breach is absolutely critical in terms of communicating with the authorities, businesses, and regulators as well as protecting your reputation. Businesses and suppliers

must work quickly to identify the source of unwanted activity and contain it, in order to determine the full extent of a breach and prevent the incident occurring again.

6) Be transparent & act swiftly

If a security breach occurs, make sure your clients hear it from the horse's mouth. It's critical you immediately notify stakeholders of potential security breaches and what action is being taken. Disclosing security compromises quickly

and honestly will help maintain trust with organisations.

Good information governance continually ensures an information supply that is:

- Trusted (accurate, complete, insightful and timely)
- Protected and secure
- Compliant with regulations
- Efficiently managed throughout its lifecycle

7) Write an audit plan - REVISIT & REVIEW REGULARLY

Appoint an internal auditor; give them the power, time and budget to manage an ongoing audit process and the audit staff necessary. Review meetings amongst Operational staff should be held quarterly and reported and discussed at a Board level annually. An audit plan details your objectives and should include an understanding of the business, the potential audit risks, a basic framework for how the resources are to be distributed and how the procedures are to be performed.

8) Certify

The single best way to reassure clients is to gain data security certifications such as ISO 27001 Security Management Standard or the Direct Marketing Association/BSI DataSeal.

For more information or a free demonstration of how MarketDeveloper could improve your security contact us now on:

PHONE: +44(0)1784 432082

EMAIL: enquiries@marketdeveloper.com