Storing and Encrypting Personal Data

Contents

The Basic Rules

The most basic rules for storing data are contained in the ***Data Protection Act, 1998*** (DPA) in UK law. This act also encompasses the ***EU Data Protection Directive (1995).*** Comply with the Data Protection Act and there should be no compliance problems. Virtually every business is a "data controller" (as defined under the Act) has to be registered under the DPA. The DPA is administered by the *Data Commissioner*.

The DPA applies to "Personal Data", i.e. data on living, identified or identifiable individuals. This is often called Personally Identifiable Information (PII). It includes names, addresses, bank account details, passport and National Insurance (NI) details. In essence, any information that can be used in the identification of a person. The more sensitive the data the higher the level of protection required. In many ways, just "common sense". The rules on holding Credit Card information are basically the same as for other PII data but is defined under the ***Payment Card Industry Data Security Standard (PCI DSS)***. These are quite simple to understand, although implementation can be demanding:

1. Build and Maintain a Secure Network
2. Install and maintain a firewall configuration to protect data
3. Protect stored data (encrypt)
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure 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 card-holder 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

For most companies handling Credit card information is so demanding it is better to delegate this to a payment gateway (e.g. PayPal or WorldPay).

Who Should Have Access to PII Data?

The Information Commissioner's Office states:

"You have the right to get a copy of the information that is held about you. This is known as a "subject access request" and each person, for which data are held, can request to see those data. It is their own data. They cannot request to see data from other people.

For staff in a company holding PII data the rule is a "need to know". Simply:

Staff Designation	Need to know?
Board level director	NO
Executive director	NO
Non-executive director	NO
CEO	NO
CIO	NO
Company Owner	NO
IT Manager/Head of IT	Perhaps, not normally
Database Administrator (DBA)	YES, but only for non Sarbanes-Oxley (2002) data
Financial Accounts Staff	Some data, mainly Sarbanes-Oxley (2002) data. NO for other data.
Data staff (customer facing staff)	YES, but only for non Sarbanes-Oxley (2002) data and only for customers they are dealing with.
Security staff	NO.
Auditors	YES
IT Developers	NO
General IT staff	NO

The Sarbanes-Oxley act (2002) is U.S. legislation (generally known as the SOX Act) that was introduced to prevent a repetition of the Enron and WorldCom scandals. Although this is American legislation it has been adopted by the F.C.A. (the UK financial regulator) and in the UK no sensible company ignores it.

Those people who do not "need to know" should not have access to the data (c.f. the DPA).

How Long can PII Data be held?

The DPA states that information should be kept for "no longer than is necessary". That is not really very helpful. Case law (cases which have processed through the courts) does help, and as a general rule when personal information is no longer being actively used it should be deleted.

What Could Happen if PII Data are not Protected?

Organisations that fail to protect PII data of employees, members of the public or customers risk very significant financial cost.

The Data Protection Compliance Report revealed that, for the period of 22 months from January 2013 to October 2014, the ICO issued £2,170,000 in fines. That does not include civil compensation!

What Needs to be Protected?

Personally Identifiable Information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can also be considered PII.

- Can a living individual be identified from the data, or, from the data and other information in your possession, or likely to come into your possession? If **NO** then probably **not** PII
- Does the data "relate to" the identifiable living individual, whether in personal or family life, business or profession? If **NO** then probably **not** PII
- Is the data "obviously about" a particular individual? If **NO** then probably **not** PII
- Is the data "linked to" an individual so that it provides particular information about that individual? If **NO** then probably **not** PII
- Is the data used, or is it *to be used*, to inform or influence actions or decisions affecting an identifiable individual? If **NO** then probably **not** PII
- Does the data have any biographical significance in relation to the individual? If **NO** then probably **not** PII
- Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event? If **NO** then probably **not** PII
- Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity? If **NO** then probably **not** PII

From the above (from the DPA) we can establish simple rules:

Data Item	PII Data?	Should Encrypt	**MUST** Encrypt
Name details	YES	YES	NO
Address details	Only when linked to a person	YES	NO
Email address	Probably not under the DPA	NO	NO
Car Registration	YES	YES	NO
Passport Number	YES	YES	YES
Passport scan or photograph or scan	YES	YES	YES
Driving license number	YES	YES	YES
Driving license photograph or scan	YES	YES	YES
NI Number	YES	YES	YES
Credit Card Details	YES	YES	YES
Bank Account Number	YES	YES	YES
Sort Code	Only if linked to Bank account	YES	NO
Tax details	YES	YES	YES
Payroll details	YES	YES	YES
Sexual preference or orientation	YES	YES	YES
Qualifications	Only if sensitive	NO	NO
Employment history	Only if sensitive	NO	NO
Employment references	YES	YES	YES

What Database Systems have Suitable Encryption

Looking at the major database systems only:

Database System	Suitable Encryption?
Microsoft SQL Server 2000 and below	NO or weak
Microsoft SQL Server 2005 and above	YES
Microsoft SQL Server Express	YES
Microsoft Access	Weak but yes
ORACLE 6 and below	NO or weak
ORACLE 7 and above	YES
ORACLE Express	YES
IBM DB2	YES
IBM UDB	YES
Teradata	YES
Ingres	YES
Sybase	YES
Hadoop	Can be
MySQL	NO
PostgreSQL	NO
MongoDB	NO
Firebird	NO
MariaDB	NO
SQLite	NO

The rule is simple. If in **red** in the table above – **DON'T USE! REALLY DON'T USE!** If you are using one of these systems, then you need to move your data off ASAP.

Encryption

There are two main types of encryption, symmetric and asymmetric. Both use one or more passwords (key) and both convert "plain text" (unencrypted) into "cypher-text" (encrypted).

With Symmetric encryption both the reader and the writer have the same password. Being in possession of the password means the encrypted data can be decrypted.

With Asymmetric encryption and "public key" is literally opened to the public. That key can only be used to encrypt data. It can safely be put into the public domain as it is useless for decryption. To read the data a "private key" is required. That will only permit decryption data and cannot encrypt.

How should we encrypt it?

The more sensitive the data the greater the need for encryption.

Entire databases can be encrypted, or columns within tables, or both (super-encryption). Most of the mainstream database systems permit both columnar and full database encryption.

The next problem is to what standard should you encrypt? Any encryption is better than none, but some are definitely better than others:

Encryption Algorithm	Type	Strong or Weak
DES	Symmetric	WEAK
Triple DES	Symmetric	INTERMEDIATE
AES	Symmetric	STRONG
RSA	Asymmetric	STRONG
Blowfish	Asymmetric	STRONG
Twofish	Asymmetric	STRONG
Threefish	Asymmetric	STRONG
Elliptic Curve Cryptography	Asymmetric	VERY STRONG
RC5	Symmetric	STRONG
IDEA	Symmetric	STRONG

With the exception of DES, all the above methods will prove entirely suitable for the encryption of PII data – providing the key length (password complexity) is sufficient. This is a specialist field, and it is generally best to leave this to specialists to manage.