Sennet Professional Indemnity Limited
5 – 7 Prospect Road
Hythe
Kent, CT21 5NS
Tel 01303 898 428
Fax 0870 974 0878
E : insure@sennetpi.com
www.sennetpi.com

A review of GDPR impact

GDPR (General Data Protection Regulation) will affect all businesses in the UK and the EU when it comes into force in May 25th this year.

Here at Legalrisks, we are getting an increasing number of calls asking our advice and recommendation. We are NOT GDPR experts but in an attempt to at least set out some basic guidelines, we have compiled the information below from a number of sources to help. We strongly recommend that you seek professional GDPR advice before May 2018 and should perform an internal GDPR audit across your own business to ensure compliance.

- To store information about an individual you must have their express permission. This permission needs to be provable if audited, so direct verbal consent is not sufficient unless the conversation is recorded and stored. This enters other areas of information capture which requires legal advice. Implied consent such as " if you do not tick this box etc " is not sufficient. Really the express permission should be expressed by a hand signed and dated agreement.

- Consent must be "freely given, specific, informed and unambiguous." This means an increased responsibility to keep records of such consent and how it was obtained. You may find you are asked to prove it (especially if these new laws increase people's general propensity to complain about personal data privacy).

- The amount of data classified as "Personal" has been broadened to also encapsulate factors such as genetic, cultural and social identity. Even an IP address can now be considered "personal data".

- Even if your company is not in the EU, if it trades within any party in the EU it will be bound by the GDPR regulations. This also applies to any parties you use that may be based outside the EU.

- Data can only be stored for a "reasonable" amount of time. This will vary depending upon your type of business. Both electronic and paper data is bound under the GDPR rules.

- If you use 3rd parties to process any data containing personal information, these processors will now have a direct legal obligation to comply with GDPR regulations even if based outside of the EU. You may hold contingent liability.

- Data held about an individual must, upon their request, be capable of being formatted and electronically transmissible to another system. This also includes the right of erasure and also details of data profiling.

- Data can only be collected that is necessary to fulfil a specific purpose and then discarded when it is no longer required.

- The penalty for breaching GDPR can by up to 4% or Euro 20M whichever is the greater of your worldwide revenue.

These are just a few of the salient points, each has reams of official regulation attached.

To summarise:

1. **To store an individual's information, you must have their express consent**
2. **You must be able to prove that consent has been given**
3. **You can only store this information for a period that is related to the reason for capturing the information**
4. **You must be able to format and transfer this information at the individuals request**
5. **You must be fully accountable for the information held and ensure any 3rd parties used in the storage or transmission of this data have taken sufficient action to comply with GDPR rules.**

In theory, the GDPR regulations are very good and are needed, however the implementation and the impact on companies, especially small business, we feel has not been thought through carefully.

- Every system and database within an organisation that contains an individual's details, even just their name or email address, must be modified or linked to a central management system that can track when express permission was received and link to the actual, or copy of, that express permission .

- If in the natural coarse of daily business an email is received from an individual at a customer, you must get their permission to keep those details e.g. an accounts department person sends an acknowledgement of payment. Otherwise the information must be deleted.

- If you receive a business card directly from an individual, you must get their express permission before you store or use that information.

- Before an order is taken over the telephone, express permission must be received to capture and store information about the order.

- You cannot perform targeted marketing to an individual without their prior express permission.

From an Insurance Point of view for Professional Indemnity Insurance (Pi)

You owe a civil liability duty of care to your clients to ensure that the data you hold about them is processed with appropriate security measures in place.

GDPR places another level of responsibility on to of this in that it now requires you expressly have that client's permission to hold data and that that data MUST conform legally required security standards.

So what is covered

Loss of Documents is a civil breach and most Pi policies will cover this to a prescribed limit set out in the policy wording. These clauses will become more restrictive in cover.

Most policies have some form of cover for breach of, or misuse of confidentiality or any right to privacy. This aspect of cover will be far more tightly controlled.

Fines and Penalties are not covered and unless it is specifically agreed that breach GDPR is catered for under the policy it is unlikely any cover, either defence of or award against the insured will be covered.

There may be a small amount of cover for Information Commissioners Office investigations under the adjudication arbitration prosecution costs clauses but this will be tightened or excluded in the future.

If your policy contains a criminal defence clause such as HSE defence covers that is unlikely to respond to any GDPR breach criminal or quasi criminal defence or fine.

Does a Legal Expenses policy cover this?

There may be some very limited costs of defence cover arising from Criminal Prosecution Defence Clauses and Data Protection and Information Commissioner clauses but in general we have found these Legal expenses policies to be unreliable and certainly fines and penalties are not covered.

Does Directors and Officer insurance cover this?

It is unlikely that D & O insurance will cover this unless specifically amended so to do as an extension to the ordinary policy.

The duty of the Director to the company and shareholders would be breached by the failure of the firm to properly effect the GDPR roll out but the resultant fine does not sit under the D & O policy directly - the diminution of company value by goodwill loss or share price slip would entail a legal action against the directors and officers and the D & O would only provide defence costs. Fine and penalties are not usually provided for nor trading losses.

Can I buy insurance specifically for GDPR losses?

Yes there are already stream of sites offering this cover. But.

The But is that the extent of the insurance is still not clear.

The policy wordings vary from 'after the event' costs recuperation, not the fines themselves but the recuperation of the costs of defending yourself only after you have paid out, to, capped loss sums under Cyber Liability policies.

There is increasing concern as to whether the fines imposed by the regulator will be insurable, either via a company's professional indemnity policy or a cyber specific policy.

Normally the insured cannot seek cover under their policy if the claim is based on the insured's own illegal acts – which a breach would constitute – so cover is offered with one hand and denied with another.

The Jury as they say is Out on this one!

This article has been compiled as a general market overview and is not a definitive legal review.
The article was written by Paul James – Sennet Professional Indemnity Limited and Nigel Park – TPS Consulting Limited, CRM ERM specialists.

Sennet Professional Indemnity Limited are the Appointed Professional Indemnity Insurance brokers for
The Association for Project Safety