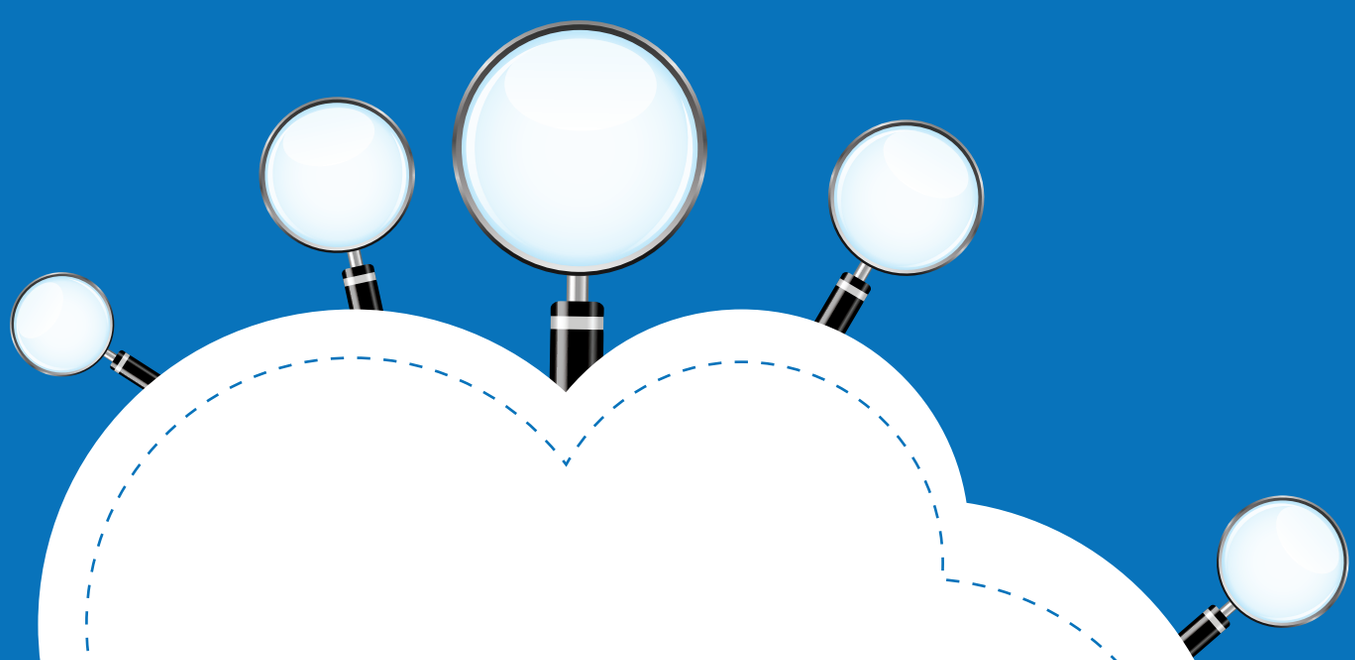
WATERFORD TECHNOLOGIES

WHAT YOU NEED TO KNOW TO MANAGE EMAIL IN THE WORKPLACE FROM A LEGAL PERSPECTIVE



INTRODUCTION

The objective of this White Paper is to outline the key legislation in managing email in the workplace & the practical solutions that Employers can implement to ensure your Organisation is compliant.

"email remains the go-to form of communication in the business world." In 2014, the report said, business email accounts are expected to total 974 million mailboxes. The report also noted that business email generates the majority of email traffic, with more than "100 billion emails sent and received per day."

The Radacti Group

"60% of business critical information is now stored, sometimes exclusively, in email."

The issues which have occurred in the workplace have been well documented, just to recap; protecting both you and your business from email misuse and its subsequent damage requires more than an email policy.

- 27% of Fortune Global 500 companies have had to deal with harassment claims concerning email (IDC).
- 30% of organizations with more than 1,000 workers employ staff to monitor outbound E-mail (Forrester)
- 42% of organizations with more than 20,000 workers employ staff to monitor outbound E-mail (Forrester)
- 56% of FTSE 1000 companies experienced email abuse
- 62% of FTSE 1000 companies had employees distributing offensive email

One survey found that even two years after the implementation of strict rules regarding the processing of emails 70% would open email they suspect to be inappropriate and, even worse, that 42% would circulate the offensive material to colleagues and friends. This can incur liabilities for employers, often at considerable expense, both financial and reputational. As can the transmission of defamatory statements by employees from their employers email addresses.

Personal data is now protected in most Countries. It includes information not only about your employees, but also about your customers and clients, or indeed often anyone else with whom your company has had dealings with in the course of business activities. This data must be stored and protected in a manner that complies with the law. The unauthorised release of information by email presents a real problem for employers. Accordingly it is necessary for employers to ensure that all employees understand their obligations and risks to the business of breaching the law regarding personal data. Breaches of the relevant legislation can lead to substantial financial penalties. If an authorised officer of the company can be proved to have acted 'recklessly' or 'with connivance' then such a person can be held personally liable. The reputational damage to a business can be devastating and have far greater long term damage to the finances of a company than the fines a Court will impose. Further, such action may lead to expensive, and damaging, civil actions if a third party has suffered loss, or damage, or distress by the breach.

In the Republic of Ireland the office of the Data Protection Commissioner was established under the 1988 Data Protection Act. In 2003 the Data Protection Amendment Act was passed which updated the 1988 legislation, implementing the provisions of EU Directive 95/46. The 1988 Act in Ireland and the UK Data Protection Act (which came into effect within days of one another) were designed to give effect to a Convention with regard to the protection of individuals in respect of the processing of personal data entered into by all EU states on 28th January 1981. As their aims were dictated in large measure by the 1981 Convention the statutes are similar.

In the Republic of Ireland the Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the 1988 and 2003 Acts, and enforcing the obligations upon data controllers. The Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.

On 6th October 2014 at Bray District Court in Ireland the first prosecutions to be completed by the Data Protection Commissioner against private investigators for breaches of data protection legislation were concluded.

The case concerned breaches of Section 22 of the Data Protection Acts, 1988 & 2003 for obtaining access to personal data without the prior authority of the data controller by whom the data is kept and disclosing the data to another person and in respect of two company directors, breaches of Section 29 of the Acts relating to the director's part in the offences committed by the company.

This Section provides for the prosecution of company directors where an offence by a company is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of the company directors or other officers. Substantial fines were imposed by the Court and case involved the first occasion on which company directors have been prosecuted by the Data Protection Commissioner for their part in the commission of data protection offences by their company.

In a media statement released following the hearing the Data Protection Commissioner stated that the case sends out a number of 'strong messages' In the first instance, it sends a strong message to private investigators and tracing agents to comply fully with data protection legislation in the conduct of their business and that if they fail to do so, they will be pursued and prosecuted for offending behaviour.

Secondly, it serves to remind all companies and businesses who hire private investigators or tracing agents that they have onerous responsibilities under the Data Protection Acts to ensure that all tracing or other work carried out on their behalf by private investigators or tracing agents is done lawfully. Specifically, in this regard, those operating in the credit union, banking, financial services, legal and insurance sectors should take note of today's proceedings and review their engagement of private investigators and tracing agents to ensure they have fully safeguarded all personal data against unlawful forms of data processing.

Thirdly, the outcome of these proceedings sends out a strong warning to directors and other officers of bodies corporate that they may be proceeded against and punished in a court of law for offences committed by the body corporate.

Finally, the findings of the investigation carried out in this case exposes the constant threat to the security of personal data which is in the hands of large data controllers and the vigilance which is required by front-line staff at all times to prevent unlawful soliciting of personal data, in particular by means of telephone contact, by unscrupulous agents. Data controllers across the State should regularly review their data protection procedures to maximise the effectiveness of their security protocols in order to counter such criminal activity.

They must ensure that all staff, and particularly those at the front-line who handle telephone calls, are fully trained in the security protocols in order to be able to recognise and deal with the threat of information blagging or pretext calling if it arises.

On Tuesday 14th October 2014 President Michael D Higgins signed the new Freedom of Information Act into law.

The FOI Act 2014 gives people a right of access to records held by many public bodies including Government Departments, the HSE and Local Authorities. Voluntary hospitals, major providers of services to people with disabilities, some broadcasters and third level bodies also fall under the Act – as does Irish Water.

The new law extends the scope of FOI legislation to cover limited areas of An Garda Síochana, the Central Bank and refugee agencies, as well as NAMA, the NTMA and the National Pension Reserve Fund. In most cases, public bodies must give their decision on an FOI request within 4 weeks of receiving it. The Office of the Information Commissioner reviews these decisions. The Information Commissioner criticized public bodies last year for failing to comply with statutory obligations set out under the Freedom of Information Act saying lack of staff resources are no excuse for FOI delays.
More information available here.
http://www.thejournal.ie/freedom-of-information-act-1726365-Oct2014/?utm_source=email

January 2014

Basis Yield Alpha Fund v. Goldman Sachs Group, Inc et al,
New York State Supreme Court, New York County, No. 652996/2011

Lawsuit filed to recoup $67m losses and $1 billion punitive damage

Goldman kept marketing Timberwolf a collaterized debt obligations even after Thomas Montag, an executive who is now Bank of America Corp's co-chief operating officer, called Timberwolf "one shitty deal" in an email to a colleague.

Link: http://www.reuters.com/article/2014/01/30/us-goldman-basisalpha-idUSBREA0T1VN20140130

REGULATION

Many organisations have implemented email monitoring systems. They are regarded properly as being essential by many businesses. When drafting and implementing such systems it is important for all companies to understand the framework of legislation that governs electronic monitoring.

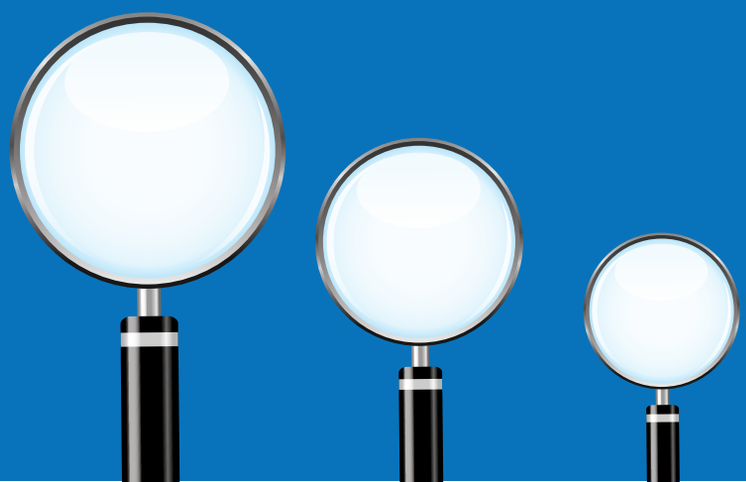
The obligations imposed on data controllers in the Republic of Ireland to ensure that data is processed in accordance with the legislation are as follows:

1. Obtain and process the personal data fairly.
2. Keep the personal data only for one or more specified and lawful purpose.
3. Process the personal data only in ways compatible with the purposes for which it was given to the data controller initially.
4. Keep the personal data safe and secure.
5. Keep the personal data accurate and up to date.
6. Ensure that the personal data is adequate, relevant and not excessive.
7. Retain the personal data for no longer than is necessary for the specified purpose or purposes.
8. Give a copy of the personal data of an individual held to that individual, should he request it.
9. Ensure that there are adequate security measures in place to:
   - (i) prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of the data (especially where the processing involves transmission over a network); and
   - (ii) ensure protection of the data against all unlawful forms of processing.

Further it should be noted that personal data is not considered to be processed fairly, under section 2D of the Act, unless the data controller ensures that data obtained from the data subject has been provided with at least the following information:-

1. The name of the data controller.
2. The purpose for collecting the data.
3. The identity of any representative nominated for the purposes of the DPA.
4. The persons or categories of persons to whom the data may be disclosed.
5. Whether replies to questions asked are obligatory and if so, the consequences of not providing replies to those questions.
6. The data subject's right of access to their personal data.
7. The data subject's right to rectify their data if inaccurate or processed unfairly.
8. Any other information which is necessary so that processing may be fair, and to ensure the data subject has all the information that is necessary to be aware as to how their data will be processed.

Employers must adhere to these principles in dealing with personal information. Any monitoring of emails must be fair and lawful and comply with the principles. Organisations should be aware that individuals are entitled to a copy of any information about them which has been collected through any form of monitoring.



PRACTICAL SOLUTIONS

1. Impact Assessments

The Code suggests that organisations undertake "impact assessments" in order to identify:

1.1 the purpose behind any monitoring;

1.2 the benefits envisaged from the monitoring;

1.3 whether any alternatives are available to achieve the same aim; and

1.4 whether the monitoring is justified.

October 2014

Currently in Pennsylvania Hundreds of pornographic and racy emails were exchanged between dozens of state government employees and officials from 2008 to 2012. The vast majority of those emails were sent or read on state email accounts. Thus far, the names of eight former employees of the attorney general's office have been released as being involved in the email exchange, and two people have already resigned from their positions.

Link: http://abovethelaw.com/2014/10/supreme-court-justice-involved-in-porngate-scandal/

2. Policies

Organisations should create policies on email use which may be incorporated into wider IT or security policies. An organisation's email policy should include:

2.1 how the email system may be used and restrictions placed on use of the system;

2.2 what personal use will be tolerated and what will not;

2.3 what information will be considered offensive and/or unacceptable for transmission via email;

2.4 if monitoring will take place, then the circumstances when such monitoring will take place;

2.5 details of how information obtained from such monitoring will be stored and used; and

2.6 how long email records are retained and the reasons for the retention of those records.

Where possible, employers should ensure employees sign up to the terms of such policies to show their consent to the monitoring taking place. This should not create any practical problems for employers. Where possible should read ALWAYS. Doing so eliminates numerous potential future difficulties and if one has taken the decision to draft and implement an email usage policy it is an act of supreme folly not to sign up one's employees to it!

Employee contracts should include provisions to state that the organisation's policies are fundamental to the employer's business and must be adhered to at all times. Failure to adhere to policies should be specified to be a breach of the employees' terms and conditions of employment which could lead to dismissal on the grounds of misconduct. Procedures should be implemented by employers for employees to ask questions about any email policy in operation.

3. Training and Awareness

Employees should be made aware of the legislation to which the employer must adhere and employers should use training sessions to increase employee awareness. Employees should be encouraged to realise their personal responsibilities under the DPA, particularly those who deal with personal information on a regular basis.

4. Data Protection Officer

A point of contact should be set up within an employer's organisation to deal with employee DPA related issues such as monitoring and to take responsibility for staff training and awareness. This point of contact may be the nominated data protection officer(s) who also should be given responsibility for ensuring that the organisation's data protection notification is up to date and covers any monitoring activities.

5. Security

Personal information, including that obtained through monitoring, should be held securely. Organisations should regularly review the adequacy and appropriateness of their IT security systems as well as "off line" security procedures. Restrictions should be placed on the number of employees who have access to personal information held by the organisation, including information obtained through monitoring.

6. Approach to Monitoring

It is clear from the legislation and in particular the Code that the less intrusive the monitoring the more likely it is that the monitoring will be justifiable. Employers must therefore balance their requirements against those of their employees and adopt a pragmatic approach to monitoring. Employers should recognise that errors do occur and employees may inadvertently access material inappropriate to the nature of the organisation or send emails without intending to do so.

June 2013

Australian Army stands down personnel over explicit emails and images sent. Three senior personnel have been stood down and 17 more are under investigation. The investigation was triggered because of a previous incident in 2011.

Link: http://mobile.abc.net.au/news/2013-06-13/lieutenant-general-david-morrison/4751800

Organisations should consider the viability of introducing automated systems for monitoring. These are generally considered to be less intrusive than manual monitoring systems. Automated systems can be used to undertake restricted pre-programmed monitoring activity. Software also exists which possesses a filtering device, which can be used to block inappropriate material from entering an organisation by email, removing the need for individuals to carry out checks. Monitoring email traffic or subject headings rather than content may provide the information sought without a high degree of intrusion.

Employers must encourage their employees to identify emails as being personal in the subject heading. This helps employers to avoid opening personal emails accidentally. Emails marked personal should only be opened in very exceptional circumstances, for example, where serious crime is suspected.

Where email accounts are required to be accessed in the absence of employees, employees should be informed that this may happen.

All emails sent by an organisation should notify users of its email system that their communications using that email system may be monitored.

What Should I do Now

The steps that are suggested here are relatively simple to implement; they are not expensive; and they address the important matters that your business should have regard to when drafting and implementing an email usage policy.

1. Conduct an impact assessment to determine the effect of monitoring on your employees and decide on the appropriate approach for your organisation to monitoring.
2. Develop an email policy covering the areas set out in this document.
3. Communicate the email policy to your employees and obtain the employees' acceptance of the policy.
4. Train employees on email usage and include email usage as part of the induction process for new employees and as part of the ongoing appraisal process.
5. Enforce and police the email policy. Not only is there little purpose in having the policy if it is not enforced but more importantly failure to do so will render it ineffective.
6. Consider which monitoring tools are appropriate for your business.
7. Regularly review and update the email policy to ensure it complies with applicable law and regulation as it changes. Any changes to the policy should also be communicated to and accepted by employees.

Remember that introducing a policy that complies with the legislative framework has immense benefits for your company. It will increase the trust and confidence of your employees by creating an open atmosphere where every member of the organisation is aware of their obligations and duties in a totally transparent manner.

There will be no mystery regarding your employment practices. It will also encourage good housekeeping and will lead to your company making potentially significant savings by disposing of out-of-date information, the freeing up of both physical and computerised filing systems and making valuable information easier to find. It may well protect your organisations from legal action. Many legal challenges will be answered by demonstrating that the policy in force complies with all relevant legislation and was at all times policed and enforced.

The policy will encourage workers to treat customers' personal data with respect as it will create a general level of awareness of personal data issues, helping to ensure that information about customers is treated properly. The Code was produced in the light of EC Directive 95/46/EC. Accordingly a policy that is compliant with the code will assist your businesses compliance with the policies and practices in other countries. The code was drafted to be in line with data protection law in other European Union member states.

Further the policy will help to prevent the illicit use of information by employees. By informing them of the principles of data protection, and the consequences of not complying with policy (and thereby the relevant legislation) employees should be discouraged from misusing information held by your organisation.

If you would like to find out how you can take action to secure your email system, make it compliant with legal requirements and implement an email policy please contact advice@waterfordtechnologies.com or

OR COPY LINK
http://www.waterfordtechnologies.com/secure-your-email

Sources:

Paper Updated by: Donal McGuire, Barrister. 10th October 2014.

Original Paper: Email Monitoring in the Workplace written by Robert Muckle Solicitors, 2003.

Waterford Technologies
Confederation House
Cork Road
Waterford

Phone: (0)51 334 967
Email: salesemea@waterfordtechnologies.com