

## 2010 PROTECTYOURDATA.IE DATA PROTECTION SURVEY

### INTRODUCTION

As Jan 28<sup>th</sup> was Data Protection Day 2010, protectyourdata.ie conducted a survey to gain a better understanding of the knowledge that businesses and organisations have of the Data Protection Acts and what they are doing to ensure compliance with the Acts. The survey was mainly targeted at small businesses with 65% of respondents having between 1 to 5 employees.

protectyourdata.ie is a new business that offers services in the area of data protection such as consultancy, training, encryption software, online backup as well as data erasure and data recovery software – all vital elements in any business' compliance with the Data Protection Acts.

### PROTECTYOURDATA.IE ANALYSIS

There is lot of information to be garnered from the survey and the following highlights the responses that protectyourdata.ie found most relevant.

Although 55% of respondents are familiar with the Data Protection Acts and the responsibilities it places on their organisations, 66% of small businesses have not implemented policies and procedures to ensure compliance. Of those that haven't;

- 18% do not have the necessary resources and expertise,
- 37% are unsure of how it applies to them
- the remaining respondents are just concerned with reducing costs and are not implementing new policies.

These figures indicate the need for these organisations to use external expertise to ensure that they are compliant with the Acts.

With regard to the knowledge of Acts, there seems to be a good understanding of some of the basic tenets with 59% of respondents knowing that you must inform an individual of the purpose of collecting the data and 92% knowing that you can only use the information for the purpose specified when it was collected.

The concern arises with regard to the possible costs associated with compliance and non-compliance with only 26% aware that the maximum possible fine on an indictable offence is €100,000. Less than half of the respondents (41%) are aware of the fact that this maximum fine can be applied to each individual record involved in the offence. Only 34% realise that they can only charge any individual €6.35 for retrieving their personal data regardless of the expense it puts on them.

One of the biggest surprises given the high profile theft of four Bord Gais unencrypted laptops is that encryption technology is still not being utilised with 63% of respondents saying that there is no encryption policy within their company for laptops, external hard disks and USB memory sticks. This figure is comparable to the figure produced by the KPMG Data Loss Barometer of 2008 that shows 62% of incidents with removable media involved data with no protection.

The use of encryption (33%) and other new technologies (USB port disabling software - 7%) lags far behind the use of antivirus software (94%) and firewalls (78%). How the figure for antivirus is not 100% is baffling considering the threat of viruses/Trojans to data on PCs and laptops.

8% of organisations have had either lost a laptop, USB memory stick or external hard disk or had it stolen. For organisations with just 1 to 5 employees this figure goes to 11%. So although approx 1 in 10 organisations will lose one of these devices, only 3 to 4 of these 10 use encryption, so the probability of a lost or stolen device being unencrypted is quite high.

Only 64% of organisations are doing a daily backup which apart from making good business sense is a vital part of any data protection policy.

Finally, the results indicate that there is a lack of knowledge with regard to the Data Protection Acts and their impact on websites and email marketing. If you collect personal details on your website then you are obliged to have a privacy statement yet 21% of respondents don't believe that they are required to. Only 9% of respondents know that you can only send marketing emails to customers (private as opposed to business) that you have made a sale to within the last 12 months. *Marketing emails can also be sent to those customers to whom you have already sent a marketing email to within 12 months of a sale in which you gave them the option to opt-out of future emails and a marketing email has been sent within every 12 month period.*

---

## SURVEY DETAILS

The survey was distributed to 593 businesses predominantly located in the west of Ireland and the midlands. A total of 35 questions were asked, though Question 35 just asked the respondent if they would like a copy of the results. The remaining 34 questions were broken down into the following sections:

- General Information (Qs 1 to 2)
- Data Protection within the organisation (Qs 3 to 8)
- Familiarity with the requirements of the Data Protection Acts (Qs 9 to 15)
- Use of websites by organisations (Qs 16 to 18)
- Storage and transfer of personal data (Qs 19 to 24)
- Software used to protect data (Qs 25 to 29)
- Backup Policies (Qs 30 to 34)

81 people participated in the survey with 49 people completing it fully. These two figures give a response rate of 13.7% and 8.3% respectively with the true figure lying somewhere in the middle, the reason for this is that there was no requirement to complete all questions which led to some questions having a higher rate of respondents than others. The actual number of respondents to each question is given in the results section.

For the purpose of analysis, we based our results on the number of responses to the particular question and made no assumptions about those that had skipped the question. Anyone else reviewing the figures is free to make their own assumptions regarding the number of respondents that skipped any particular question.

---

## CONCLUSION

Although there appears to be a good awareness and understanding of the Data Protection Acts themselves there doesn't seem to be a good understanding of how best to implement policies to be in compliance with the Acts. This lack of compliance is highlighted by the fact only 34% of organisations have implemented Data Protection policies, 62 % don't have an encryption policy and 36% are so unconcerned that they do not do a daily backup. That there is a somewhat laissez faire attitude to compliance with the Acts may be due to the fact that organisations aren't fully aware of the possible penalties associated with non-compliance with only 26% of respondents aware of the maximum fine.

Overall, there is the need for organisations to be made more aware of the finer details of the Acts whether through taking the appropriate training courses or through their own research to ensure compliance. An outlay on training and education may prevent a more costly payout due to non-compliance in the future.

**RESULTS**

Q1.

How many employees does your company have?		
Answer Options	Response Percent	Response Count
1 to 5	64.6%	51
6 to 15	20.3%	16
16 to 30	2.5%	2
30+	12.7%	10
<i>answered question</i>		<b>79</b>
<i>skipped question</i>		<b>0</b>

Q2.

What county does your business operate from?		
Answer Options	Response Percent	Response Count
Clare	3.1%	2
Donegal	0.0%	0
Galway	75.4%	49
Leitrim	1.5%	1
Longford	0.0%	0
Mayo	9.2%	6
Roscommon	3.1%	2
Sligo	4.6%	3
Westmeath	3.1%	2
Other (please specify)		16
<i>answered question</i>		<b>65</b>
<i>skipped question</i>		<b>14</b>

Q3.

Are you familiar with the content of the Data Protection Acts and the responsibilities they place on your organisation?		
Answer Options	Response Percent	Response Count
Yes	55.1%	38
No	44.9%	31
<i>answered question</i>		<b>69</b>
<i>skipped question</i>		<b>10</b>

Q4.

<b>Does your organisation have specific policies in place to ensure compliance with the Data Protection Acts?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Yes	43.3%	29
No	56.7%	38
<b><i>answered question</i></b>		<b>67</b>
<b><i>skipped question</i></b>		<b>12</b>

Q5.

<b>Is there a specific role within the organisation where Data Protection compliance is part of the remit?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Yes	19.4%	12
No	66.1%	41
Other (e.g. it is subsumed by the HR department)	14.5%	9
<b><i>answered question</i></b>		<b>62</b>
<b><i>skipped question</i></b>		<b>17</b>

Q6.

<b>Does the job description for the role in Q4 contain a detailed outline of the expectations and objectives in relation to compliance with Data Protection Acts?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Yes	21.4%	9
No	78.6%	33
<b><i>answered question</i></b>		<b>42</b>
<b><i>skipped question</i></b>		<b>37</b>

Q7.

<b>How would you rate the importance of Data Protection within your organisation?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Very Important	44.9%	31
Important	30.4%	21
Somewhat important	17.4%	12
Not important	7.2%	5
<b><i>answered question</i></b>		<b>69</b>
<b><i>skipped question</i></b>		<b>10</b>

Q8.

<b>Which of the following best describes your organisations' compliance with the Data Protection Acts?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
We have implemented policies and procedures to ensure compliance	33.8%	22
We don't have the necessary resources and expertise to ensure compliance	18.5%	12
We are aware of the Act but don't know how it applies to us	36.9%	24
At present we are more concerned about reducing costs and we are not implementing new policies and procedures	10.8%	7
<b>answered question</b>		<b>65</b>
<b>skipped question</b>		<b>14</b>

Q9.

<b>When gathering personal information from individuals what must an individual be informed of?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
The length of time the information will be kept for e.g. 7 days, 2 years etc..	22.2%	12
The security procedures used to secure the data e.g. encryption used or not	13.0%	7
<b>The purpose of collecting the data e.g. for marketing</b>	<b>59.3%</b>	<b>32</b>
The name of the person actually gathering the information	5.6%	3
<b>answered question</b>		<b>54</b>
<b>skipped question</b>		<b>25</b>

Q10.

<b>If your organisation sends marketing emails or email newsletters to individual consumers (not business customers), then, per the Office of the Data Commissioner, which one of the following is legally permissible:</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
<b>You can send it to only those individuals to whom you have made a sale within the last 12 months</b>	<b>9.1%</b>	<b>4</b>
You can send it to any email address that an individual has given to your business regardless of the reason they gave it to you	2.3%	1
You can send it any email address on a legally purchased email listing	4.5%	2
You can send it to any email address that an individual has given to your business as long as you include an opt-out option	77.3%	34
You can send it to any email address you have regardless of its source	6.8%	3
<b>answered question</b>		<b>44</b>
<b>skipped question</b>		<b>35</b>

Q11.

**If your organisation receives a request from an individual to view all the information that you hold on them, you can:**

Answer Options	Response Percent	Response Count
Inform them of the cost involved and let them decide if want to proceed	59.1%	26
Charge them a once-off fee of €150	0.0%	0
Bill them for the cost involved in retrieving the information at a rate of €12.70 per hour	6.8%	3
<b>Only charge them €6.35 in total regardless of the cost to your organisation</b>	<b>34.1%</b>	<b>15</b>
<i>answered question</i>		<b>44</b>
<i>skipped question</i>		<b>35</b>

Q12.

**Once you have gathered personal information from an individual, it can:**

Answer Options	Response Percent	Response Count
Be used for any purpose by the company that collected it	7.7%	4
<b>Be only used for the purpose specified when it was collected</b>	<b>92.3%</b>	<b>48</b>
Be transferred to any other company within your company group structure (parent/sister company) who offer the same type of products/services	0.0%	0
Be transferred to any other company who offer the same type of products/services	0.0%	0
<i>answered question</i>		<b>52</b>
<i>skipped question</i>		<b>27</b>

Q13.

**The maximum possible fine on a summary conviction for an offence against the Data Protection Acts is:**

Answer Options	Response Percent	Response Count
€1,000	9.3%	4
<b>€3,000</b>	<b>30.2%</b>	<b>13</b>
€6,350	14.0%	6
€12,700	46.5%	20
<i>answered question</i>		<b>43</b>
<i>skipped question</i>		<b>36</b>

Q14.

The maximum possible fine on indictment for an offence against the Data Protection Acts is:

Answer Options	Response Percent	Response Count
€50,000	26.2%	11
<b>€100,000</b>	<b>26.2%</b>	<b>11</b>
€127,000	21.4%	9
€250,000	26.2%	11
<i>answered question</i>		<b>42</b>
<i>skipped question</i>		<b>37</b>

Q15.

The fines referred to in Questions 12 and 13 can be applied to: (For the purpose of this question one record equates to all the personal information that is held by an organisation on one individual)

Answer Options	Response Percent	Response Count
<b>Each individual record involved in the offence</b>	<b>41.5%</b>	<b>17</b>
Each set of 1,000 records or part thereof	0.0%	0
Each set of 3,000 records or part thereof	2.4%	1
All the records – the actual number of records included in the offence doesn't matter	56.1%	23
<i>answered question</i>		<b>41</b>
<i>skipped question</i>		<b>38</b>

Q16.

Do you use your website to collect information from visitors?

Answer Options	Response Percent	Response Count
Yes	32.7%	17
No	67.3%	35
<i>answered question</i>		<b>52</b>
<i>skipped question</i>		<b>27</b>

Q17.

If you process payments on your website how long do you retain the credit card information?		
Answer Options	Response Percent	Response Count
It is deleted once the payment is processed	6.8%	3
It is deleted after 7 days	0.0%	0
We use a third party (e.g. PayPal) to process our payments and we don't know how long they keep the information for.	15.9%	7
We don't process payments on our website.	72.7%	32
We use a third party (e.g. PayPal) to process our payments and they keep the information for:	4.5%	2
		0
	<b>answered question</b>	<b>44</b>
	<b>skipped question</b>	<b>35</b>

Q18.

Do you have a privacy statement on your website?		
Answer Options	Response Percent	Response Count
Yes	26.9%	14
No	51.9%	27
No, we only collect names and contact details, we don't process payments	21.2%	11
	<b>answered question</b>	<b>52</b>
	<b>skipped question</b>	<b>27</b>

Q19.

Do you use laptops within your organisation?		
Answer Options	Response Percent	Response Count
Yes	88.2%	45
No	11.8%	6
	<b>answered question</b>	<b>51</b>
	<b>skipped question</b>	<b>28</b>

Q20.

Do you use USB memory sticks within your organisation?		
Answer Options	Response Percent	Response Count
Yes	76.5%	39
No	23.5%	12
<i>answered question</i>		<b>51</b>
<i>skipped question</i>		<b>28</b>

Q21.

Do you use external hard drives within your organisation?		
Answer Options	Response Percent	Response Count
Yes	56.9%	29
No	43.1%	22
<i>answered question</i>		<b>51</b>
<i>skipped question</i>		<b>28</b>

Q22.

Please indicate which devices are used to store or transfer personal data both internally within your organisations' offices and externally by employees working away from the organisations' offices. (Please tick all that apply)

Answer Options	Laptops	USB Sticks	External Hard Disks	None used	Response Count
1 - Within the office	25	18	21	10	48
2 - Away from the office	27	23	7	10	45
<i>answered question</i>					<b>51</b>
<i>skipped question</i>					<b>28</b>

Q23.

Has your organisation ever lost (or had one stolen) a laptop, USB memory stick or an external hard drive?

Answer Options	Response Percent	Response Count
Yes	7.8%	4
No	92.2%	47
If Yes, please specify		3
<i>answered question</i>		<b>51</b>
<i>skipped question</i>		<b>28</b>

Q24.

<b>If the device contained personal information did you:</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Inform the Data Protection Commissioner about the lost data	22.2%	2
Inform all the individuals whose information was lost	11.1%	1
Inform both the Data Protection Commissioner and the individuals concerned.	11.1%	1
Do nothing – i.e. you did not inform either the Data Protection Commissioner or the individuals concerned	44.4%	4
Change your internal policies and procedures but did not inform either the Data Protection Commissioner or the individuals concerned	11.1%	1
	<b><i>answered question</i></b>	<b>9</b>
	<b><i>skipped question</i></b>	<b>70</b>

Q25.

<b>Is it the policy of your organisation to encrypt the following: (Tick all that apply)</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Laptops	23.9%	11
USB Memory Sticks	15.2%	7
External Hard Drives	19.6%	9
None of the above there is no encryption policy	63.0%	29
	<b><i>answered question</i></b>	<b>46</b>
	<b><i>skipped question</i></b>	<b>33</b>

Q26.

<b>If there is a policy to encrypt devices, is it monitored and enforced?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Yes	30.4%	14
No	15.2%	7
There is no encryption policy	54.3%	25
	<b><i>answered question</i></b>	<b>46</b>
	<b><i>skipped question</i></b>	<b>33</b>

Q27.

<b>Which of the following technologies do you use to help protect the data that you store? (Tick all that apply)</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Anti-virus software	93.5%	43
Anti-spyware software	63.0%	29
Firewalls (either hardware or software)	78.3%	36
Encryption	32.6%	15
Software monitoring information downloaded by employees	10.9%	5
Software disabling USB ports	6.5%	3
Other (please specify)		2
<b>answered question</b>		<b>46</b>
<b>skipped question</b>		<b>33</b>

Q28.

<b>Do you have access controls in place to ensure that only those employees that need to access personal information are the only ones that can?</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Yes	73.3%	33
No	26.7%	12
<b>answered question</b>		<b>45</b>
<b>skipped question</b>		<b>34</b>

Q29.

<b>Which of the following best describes your system of access controls:</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Access to personal information is reviewed on a regular basis with access granted and revoked where appropriate	58.8%	20
Access controls have not been reviewed since initial implementation	14.7%	5
Although implemented, there is no process in place to ensure adherence	26.5%	9
Other (please specify)		2
<b>answered question</b>		<b>34</b>
<b>skipped question</b>		<b>45</b>

Q30.

Have you ever lost data?		
Answer Options	Response Percent	Response Count
Yes	43.8%	21
No	56.3%	27
<i>answered question</i>		<b>48</b>
<i>skipped question</i>		<b>31</b>

Q31.

Were you able to retrieve it from backup?		
Answer Options	Response Percent	Response Count
Yes	70.8%	17
No	25.0%	6
No, we thought it was backed up but when we went to restore it we were unable to	4.2%	1
<i>answered question</i>		<b>24</b>
<i>skipped question</i>		<b>55</b>

Q32.

Which of the best describes your backup policy?		
Answer Options	Response Percent	Response Count
Daily	63.8%	30
2or 3 times a week	0.0%	0
Once a week	19.1%	9
Every 2 weeks	0.0%	0
Monthly	4.3%	2
Whenever we think of it, could be twice a month or twice a week	12.8%	6
<i>answered question</i>		<b>47</b>
<i>skipped question</i>		<b>32</b>

Q33.

Do your regularly test your backups to ensure that you can successfully restore from them?		
Answer Options	Response Percent	Response Count
Yes	57.4%	27
No	42.6%	20
Other (please specify)		1
<b><i>answered question</i></b>		<b>47</b>
<b><i>skipped question</i></b>		<b>32</b>

Q34.

Are copies of you backup securely stored offsite?		
Answer Options	Response Percent	Response Count
Yes	58.3%	28
No	41.7%	20
<b><i>answered question</i></b>		<b>48</b>
<b><i>skipped question</i></b>		<b>31</b>