2021-09-23

Data Protection Awareness Survey of Tertiary Sector Teachers and Lecturers in Ireland

Aidan Kenny
Technological University Dublin, aidan.kenny@tudublin.ie

Data Protection Awareness Survey of Tertiary Sector Teachers and Lecturers in Ireland

Dr Aidan Kenny[i]
Data Protection Officer, Teachers' Union of Ireland (TUI)
2021

Abstract

Within the European Union all organisations and companies which process personal data must comply with the terms of the General Data Protection Regulation (GDPR) 2016 which was transposed into law in 2018. GDPR provides fundamental rights to individuals relating to the protection of personal data, the terms for processing personal data and privacy of personal data. The regulation also requires both data controllers and data processors to take an active approach to ensuring compliance and to promoting awareness of data protection. The regulation includes powers of enforcement, investigation, and sanction. The Data Protection Commission in Ireland is the independent national authority in the EU with responsibility to uphold individual rights relating to the protection of personal data.

This research paper provides insights into the level of GDPR awareness of a specific population sample of teachers and lecturers who work in the Irish tertiary education sector and are members of the Teachers' Union of Ireland (TUI). The research approach used was 'practice-based' (Eraut 2004) as a professional in the field and informed by 'workers critical research' as a worker in the sector (Kincheloe, McLaren 1994). The method included a questionnaire developed to measure levels of awareness about GDPR, it used closed choice questions and open comments boxes, and risk assessment indicators relating to remote working. The questionnaire was designed as an online survey for safe distribution during the Covd-19 restriction period. The survey items focused on GDPR key principles, rights of individuals, need to gain consent, data breach procedure and training. In addition, the survey explored experiences of GDPR issues while engaged in emergency remote working due to Covid-19 restrictions.

The online survey was distributed in February 2021 and was open for two weeks. The survey received N=502 responses, of which 39% were from Second Level Schools, 37% Higher Education , and 22% Further Education and Training. The results demonstrate a general good level of awareness about GDPR obligations, such as processing personal data, requirements for consent and confidentiality and procedures for dealing with matters that arise including data breaches. In addition, respondents indicated risk levels for GDPR concerns while remote working during Covid-19 restrictions The survey results suggest that respondents understood the importance of GDPR to protect individual rights and the necessity to have policies and procedures to achieve this obligation. Respondents indicated that training was required to keep up to date on GDPR matters and that training material should include fact sheets, short videos and online modules. It was suggested that engagement between employers and the union could assist in promoting awareness of GDPR in workplaces including emergency remote working.

Introduction

The Teachers' Union of Ireland (TUI[1]) is a registered trade union under the Trade Union Acts 1871-1990, listed in the Companies Registration Office[2], Register of Friendly Societies. TUI as a trade union is a data controller and data processer of the personal data of members for the legitimate business of the union and to provide a service to the members. TUI as a data controller and a data processor is required to adhere to the data protection laws[3]. The European Union General Data Protection Regulation (2016)[4] was transposed into Irish legislation on in May 2018. GDPR provides individuals with enhanced protections in the form of fundamental rights regarding the processing of their personal data and privacy, putting legal obligations on data controllers and data processers to ensure compliance. Data relating to trade union membership is categorised[5] as sensitive personal data requiring an additional level of protection. GDPR requires data controllers and data processers to have necessary procedures in place for compliance with the six GDPR principles.

- Lawful bases for processing data. A data processor (organisation or company) must adhere to the legal requirement of the state and EU relating to the processing of personal data of an individual. There must be a legitimate basis for the processing of such personal data. The legitimate basis relied on for processing personal data must adhere to the law and be transparent and made available. Informed consent must be obtained before data is processed.
- Specific purpose for processing data. The gathering of personal data and the processing of personal data must be done for a stated specific purpose. The purpose for processing data must be transparent and made available. The purpose used for processing data must be in compliance with the legislation of the state and EU.
- Minimisation of data. A data processor is required to only gather as much data as is necessary for the purpose and to complete the tasks and operations associated with the purpose. It is not advisable that data processors gather more data than is required and necessary to fulfil the specific purpose.
- Accuracy of data. A data processor is required to maintain the accuracy of personal data records and to update personal data on a regular or scheduled basis. Additionally, personal data should be amended where errors are brought to the attention of the data processor.
- Storage and retention of data. Data processors are required to only store data for durations that are related to the legitimate business reasons and specific purpose and operations. Personal data should not be stored for longer than required. Personal data should be securely deleted when its purpose is complete.
- Integrity, security, and access. Data processors are required to operate in accordance with the legislation of the state and EU this includes assigning a Data Protection Officer[6] (DPO), have appropriate security measures in place to protect personal data and restrict access to personal data on a need to know for operational matters.

In addition to principles, controllers and data processers have to demonstrate accountability and be proactive in GDPR compliance measures including appointing a DPO, having appropriate procedures in place, and promoting awareness of data protection matters. This includes having measures to respect the individual rights of data subjects such as:

[1] For more detailed information about TUI see website https://www.tui.ie/

[2] Companies Registration Office https://www.cro.ie/Society-Union/RFS-Trade-Unions

[3] For list of data protection laws see https://www.dataprotection.ie/en/who-we-are/data-protectioN=legislation

[4] The text of the regulation can be accessed at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[5] See seven categories of special personal data at https://www.dataprotection.ie/en/individuals/data-protectioN=basics/definitioN=key-terms

[6] The author was DPO for TUI from 2016 to 2021, returned to Dublin Institute of Technology which now a technological university (Technological University Dublin) in September 2021.

- Right to be informed. An individual has a right to request a data processor to inform them if their personal data is being processed, and if it is, what type of personal data is being processed.
- Right to access. An individual has a right to request copies of personal data relating to the individual that the data processor uses. The data process must provide the personal data requested within specific time frames and protect the personal data of others.
- Right of erasure. An individual has a right to request a data processor to delete his/her personal data.
- Right to restrict processing. An individual has a right to request a data processor to restrict access to his/her personal data.
- Right to data portability. An individual has a right to know where his/her personal data are being stored and used.
- Right to object. An individual has a right to object to a data processor using his/her personal data.
- Rights in relation to automated decision-making and profiling. An individual has a right to know how his/her personal data are used particularly in automatic processes which may inform decision making.

Data controllers and data processors are also required to have appropriate procedures to deal with any data breaches including unauthorised access, theft or loss of data, hacking, privacy breach, circulation of personal data, wrongful use of personal data. Data controllers and data processers are obliged to have the appropriate equipment, systems and security mechanism to protect personal data. This includes assigning appropriate resources to manage and organise the data processing activities used in the operations of the organisation.

The research approach used

Eraut (2004, p1) notes, 'Professional practice both generates and uses evidence'. The evidence can be used to inform practice and can contribute towards the development of procedures and polices within the profession or workplace. The evidence may be produced by the professional carrying out research or by others assigned to carry out the research task. Within academic environments it is established practice for academics to carry out research relevant to their area of specialisation and /or their institute. The research may focus on internal matters relating to the institute or external matters. In education teachers may also engage in research, usually this research is focused on school-related activities or practice. Organisations also employ researchers to explore matters of relevance to operations and products. While professional practice can generate evidence to inform practice, Kincheloe and McLaren (1994, p146) proposed that workers can be 'critical researchers' within their workplaces, adding to the '…production of more useful and relevant research on work'. This research on GDPR awareness was informed by professional-practice and worker-based research. The Data Protection Officer (DPO)[7] as a worker in TUI sought to gather information with a view to inform policy development within the workplace and contribute to professional practice within the tertiary education sector relating to GDPR. Professional practice research can contribute to the production of knowledge and evidence for use in the workplace, the profession and other interest groups ad network. This research sought to contribute toward the professional practice of members (teachers and lecturers) relating to GDPR and share knowledge gained with the network of DPOs organised by the Irish Congress of Trade Union (ICTU)[8]. The approach from

[7] For detailed information about the role of a DPO see Data Protection Commission https://dataprotection.ie/en/organisations/know-your-obligations/data-protection-officers

[8] For information about ICTU see https://www.ictu.ie/

a worker researcher perspective sought to ascertain information that was both relevant and useful to TUI its members, and to promote GDPR best practice in the workplaces.

The online survey and sample population

The purpose of the online survey was to ascertain TUI members level of awareness of the GDPR, specifically items relating to the key GDPR principles, individual rights, consent, security, training, and data breaches. In addition, the survey sought members experiences of GDPR while working remotely due to the Covid-19 emergency restrictions[9]. The survey results were to be used to inform union GDPR policy and practice. The online survey used the SurveyMonkey[10] platform to arrange survey questions, distribute the survey link, and gather responses. SurveyMonkey's GDPR compliance statement was reviewed and considered appropriate for the purpose of this survey. Once the survey closed the data extracted from SurveyMonkey was deleted from the SurveyMonkey platform. The survey was designed to respect privacy and assure anonymity. All the tracking settings were turned off. Respondents were not required to submit their email address or disclose their identity. The survey was distributed by the union's Head Office to branches in February 2021, a reminder was issued 7 days later, and the survey was closed on the 10th day. The survey population was the membership of the union in employment which is estimated to be 18,000 (not including those in the Retired Members Association or Student members). The membership can be generally categorised into three sectors: Second Level Schools[11], Further Education and Training[12] and Higher Education[13] . The survey invitation letter was distributed to the branch network for local circulation to members in each sector. This approach does not assure access to the total population and there can be local communication issues with access to lists. Considering the possible distribution limits the sampling method used could best be considered as opportune sampling or simple random sampling of a defined population. In order to have a low margin of error (3.5%) and a high confidence rate (95%) the survey sought to gain N=750 responses. However, the actual number of responses received was N=504. This provides for a moderate margin of error of 4.3% and a confidence rate of 95%[14]. Given the homogenous nature of the population in terms of role (mainly teachers and lecturers) and work location (mainly remote working due to Covid-19 Level 5 restrictions) N=504 responses are acceptable to provide a high level of confidence and a moderate margin of error for the purpose of this survey. While the sample size is accepted as the total population, the number of members who received the survey invitation letter is unknow, therefore it is difficult to calculate the response rate (Reponses as a percentage of sample size). If it is assumed that there is a likelihood that the total population (18,000 members) may have received the survey invitation email, then the response rate would be 2.8%. The survey consisted of seven sections including response profile, general principles, individual rights, consent, data breach, training, remote working. The questions include multiple choice, Likert scale and text comment boxes. In some sections several questions were clustered together. Responses to questions are presented as percentages, numbers, weighted average and Likert scales.

[9] See Gov.ie for the list of Covid-19 Level 5 Restrictions https://www.gov.ie/en/publication/2dc71-level-5/

[10] See https://www.surveymonkey.com/curiosity/

[11] These include Community and Comprehensive Schools and Education and Training Board Schools for full listings se Department of Education https://www.gov.ie/en/organisation/department-of-education/

[12] The Further Education and Training sector includes Post Leaving Certificate Colleges managed by the Education and Training Boards for information see https://www.etbi.ie/etbs/post-leaving-certificate-courses/

[13] This includes institutes of technology and technological universities https://www.gov.ie/en/organisation/department-of-higher-education-innovation-and-science/

[14] See sample size calculator https://www.checkmarket.com/sample-size-calculator/

The survey response profile

The survey requested respondents to identify their role within the union, Workplace Committee, Branch Committee, Executive Committee, Member, Member who does not process data and Other. The majority of respondents 83% identified as either Member (69.4%) or Member who does not process personal data (13.6%). The respondents identified there sectors as Second Level Schools 39.1%, Higher Education 37.1% and Further Education and Training was 22.4%. Other accounted for 1.4% (N=7) these were mainly staff who work in head office. There were also 3 missed counts, this is where the question is not answered by a respondent. The response frequency per sector is detailed in Table 1.

Sector - Please indicate which sector you work in				
		Frequency	Percent	Valid Percent
Valid	Other (please specify)	7	1.4	1.4
	Second Level Education	196	38.9	39.1
	Further Education and Training	112	22.2	22.4
	Higher Education	186	36.9	37.1
	Total	501	99.4	100.0
Missing	System	3	.6	
Total		504	100.0	

Table 1: Response frequency by sector

Survey data and clusters

The survey mainly used Closed Question format, utilising several scale options including Multiple-Choice Questions to indicate preference, General Questions to indicate Yes or No, Likert Scale Questions to indicate level of awareness (Not at all aware, Slightly aware, Moderately aware, Very aware, Extremely aware) and risk level . In addition, Open Questions were catered for in Text Box options included in some question clusters. The results are presented in the following numerical formats percentages and response number for General Questions and Multiple-Choice Questions, and weighted average and percentages for Likert Scale Questions. The index for weighted averages scores for question clusters; 1) Key principles, 2) Data access, 3) Data breach and 4) Consent, is presented Table 2.

Level of awareness	Weighted score
Not at all	less than 1
Slightly	1 or above but less than 2
Moderately	2 or above but less than 3
Very	3 or above but less than 4
Extremely	4 to 5

Table 2: Weighted score index

Cluster 1, Data protection principles

This cluster focused on the six key GDPR principles[15] relating to processing personal data including Lawfulness for gathering data, Purpose for processing data, Minimisation of data required, Accuracy of data gathered, Storage and access to data and Integrity of data including security and confidentiality. This cluster of items received N=496 responses and N=8 skipped (Non=responses).

For the item Lawful gathering of data, respondents indicated Extremely aware 37%, and Very aware 44%, only .4% indicated they were Not at all aware and 3.4% were Slightly aware. The weighted average score for this item was 4.15 (Extremely aware). For the item Purpose, personal data must be processed for a specific purpose, respondents indicated 38% Extremely aware and 42% Very aware, compared to 2% Not at all aware and 3% Slightly aware. The weighted average score for this item was 4.13 (Extremely aware). For the item Minimisation:

[15] This survey focused on six key principles relevant to the sample population there is a seventh principle Accountability, information on these GDPR principles can be obtained at https://www.gov.ie/en/organisation/department-of-higher-education-innovation-and-science/

'Only collect and process the necessary amount of data for the specific purpose' respondents indicated 39% were both Extremely aware and Very aware and only 1% indicated that they were Not at all aware and 3% Slightly aware. The weighted average score for the item was 4.12 (Extremely aware). For the item Accuracy: 'Personal data must be accurate and up to date' respondents indicated 36% Extremely aware, 35% Very aware compared to 3% Not at all aware and 4% Slightly aware. The weighted average score for the item was 3.98 (Very aware). The item Storage: 'Personal data can only be stored to fulfil the specific purpose received 39% for both Extremely aware and Very aware compared to 1% Not at all aware and 4% Slightly aware. The weighted average score for the item was 4.11 (Extremely aware). For the item, Integrity: 'Processing data must ensure security, integrity, and confidentiality', respondents indicated 46% Extremely aware, 40% Very aware, whereas only 15% indicated that they were Not at all aware and 2% Slightly aware. The weighted average score for the item was 4.27 (Extremely aware). The weighted average scores for each item in this cluster are presented in Table 3. The highest level of awareness was for the item Integrity (4.2 weighted average score) and the lowest was for the item Accuracy (3.98 weighted average score). In general respondents indicated overall high levels of awareness of the six key GDPR principles.

Please indicate your level of awareness relating to the key principles of GDPR	
Item	*Weighted average*
Lawful: Processing personal data must be done in a lawful, fair, and transparent way	4.15
Purpose: Personal data must be processed for a specific purpose	4.13
Minimisation: Only collect & process the necessary amount of data for a specific purpose	4.12
Accuracy: Personal data must be accurate and up to date	3.98
Storage: Personal data can only be stored to fulfil the specific purpose	4.11
Integrity: Processing data must ensure security, integrity, and confidentiality	4.27

Table 3 Cluster: Key GDPR principles, weighted average

The items were also explored for relationships based on Sector, by using crosstabulation including Pearson's Chi-square (r)[16]. This provided an insight into whether the respondents in each sector shared similar levels of awareness to the items.

There was a similarity in responses within the Sectors to the item, Lawful processing of data, with 'Very aware' identified as the highest level of awareness (Second Level Schools N=78, Further Education and Training N=52 and Higher Education N=87) and 'Extremely aware' identified as the second highest level of awareness (Second Level Schools N=68, Further Education and Training N=44 and Higher Education N=69). In terms of relationship between sector responses there was a strong positive level of significance at r=.637. For the item, 'Process personal data for a specific purpose', there was similarity in responses received from the three main sectors, each sector identified 'Very aware' as the highest (Second Level Schools N=76, Further Education and Training N=50 and Higher Education N=81) and 'Extremely aware' was the second highest in the three sectors (Second Level Schools N=69, Further Education and Training N=50 and Higher Education N=70). The level of relationship between sector responses was a low positive at r=.222. Regarding the item, 'Minimisation: only collect and process the necessary amount of data for the specific purpose', there was similarity between the Further Education and Training, and Higher Education sectors both indicating the Very aware as the highest level (N=51 and N=75) and the second highest level as extremely aware (N=46 and N=74). Whereas the Second Level indicated the reverse with Extremely aware at N=71 and Very aware N=68. There was a very low positive level of significance at r=.086. For the item,' Accuracy: Personal data must be accurate and up to date', there was some similarity between responses in the three sectors. Both Second Level and Further Education and Training indicated Extremely aware as the highest level (N=68, N=52)

[16] Pearson Chi-square (r) is a statistical test for difference or similarities ('goodness of fit') between variable frequencies, 0.0 means there is no statistical significance, 1.0 denotes a perfect positive level of significance and -1.0 is a perfect negative level of significance.

and Very aware as the second highest (N=66 and N=42) whereas, Higher Education indicated the reverse with Very Aware at N=62 and Extremely aware at N=58. The was a very low level of statistical significance between the sectors and the item at r=.058. Relating to the item, 'Storage: personal data can only be stored to fulfil the specific purpose', there was similarity between responses from sectors, both Further Education and Training and Higher Education identified the highest level as Very aware (N=50, N=76) whereas Second Level Schools identified Extremely aware (N=75). There was also a large grouping in the Moderately aware position (Second Level Schools N=35,Further Education and Training N=11 and Higher Education N=26), see Figure 6. The relationship between sectors was moderate positive at r=.489. The item, 'Integrity: Processing data must ensure security, integrity and confidentiality' when tested with Sectors, showed a degree of similarity in responses. Both Second Level Schools and Further Education and Training identified Extremely aware as the highest level (N=86 and N=57), while Higher Education identified Very aware as the highest level (N=81). The level of relationship was moderate positive at r=.510. From the data there is a good positive relationship between the sectors responses to the six items, the item Accuracy has the smallest relationship at r=.058 while Lawful processing had the highest at r=.637.

Cluster 2, Data access

This cluster sought to gain respondents awareness of individual rights[17] under GDPR. The cluster contained seven items relating to individual rights regarding personal data such as, to be informed if personal data is used, be informed what types of personal data are used, to gain copies of the data, to object to the use of the data, to have the data amended, to have the data deleted and to restrict access to the data. The cluster received N=499 responses and N=3 skipped (Non-responses). Regarding the item, 'To be informed if their individual personal data is used', respondents indicated 37% Extremely aware, 31% Very aware compared to 3% Not at all aware and 6% Slightly aware. The weighted average score for the item was 3.9 (Very aware). For the item, 'To be informed what type of personal data is used', respondents indicated 35% Extremely aware, 31% Very aware whereas 6% indicated they were Not at all aware and 5% were Slightly aware. The weighted average score for the item was 3.8 (Very aware). With reference to item, 'To gain copies of the personal data used', 39% of respondents indicated Extremely aware and 30% Very aware in comparison to 4% Not at all aware and 6% Slightly aware. The average weighted score for the item was 3.9 (Very aware). Item, 'To object to the use of their personal data', received 35% Extremely aware and 26% Very aware and at the other end of the scale 6% indicated they were Not at all aware and 8% were Slightly aware. The weighted average score for the item was 3.7 (Very aware). For item, 'To have the personal data corrected', 38% indicated Extremely aware and 28% were Very aware while 5% were Not at all aware and 6% were Slightly aware. The weighted average for this item was 3.8 (Very aware). Relating to item, 'To have the personal data deleted', the respondents indicated 32% Extremely aware, 23% Very aware as compared to 11% Not at all aware and 8% Slightly aware. The weighted average score for this item was 3.5 (Very aware). The item, 'To restrict the use of the personal data', received 34% Extremely aware, 24% Very aware while 8% were Not at all aware and 9% were Slightly aware. The weighted average score for this item was 3.6 (Very aware). There was a good general level of awareness of the items in this cluster, the highest weighted average score was for the item, to gain copies of data (3.9) and the lowest was (3.5) for the item relating to deleting data. A Bar Chart of the Cluster and items with weight averages is presented in Table 4 below.

[17] More information on individual rights can be found on the Data Protection Commission website at https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation

Are you aware that an individual has a right to request and receive the following information from an organisation that processes personal data?	
Item	*Weighted average*
To be informed if their individual personal data is used	3.92
To be informed what type of personal data is used	3.85
To gain copies of the personal data used	3.93
To object to the use of their personal data	3.78
To have the personal data corrected	3.88
To have the personal data deleted	3.58
To restrict the use of the personal data	3.67

Table 4 Cluster: Individual rights, weighted average

For the item, 'To be informed if their individual personal data is used', there was similarity in responses received from the sectors. All sectors identified the highest level as Extremely aware (Second Level Schools N=72,Further Education and Training N=50 and Higher Education N=63) and the second highest level as Very aware (Second Level Schools N=65,Further Education and Training N=34 and Higher Education N=56). There was a moderate level of statistical significance at r=.516. There was a degree of similarity between sector responses to item, 'To be informed if their individual personal data is used'. Both Further Education and Training and Higher Education identified the highest level as Extremely aware (N=48, N=61) and Very aware as the second highest (N=32, N=52). Second Level identified Very aware as the highest level (N=68) and Very aware as the second highest level (N=68). The level of relationship was a strong positive significance at r=.731. There was good similarity between the sectors relating to the item, 'To gain copies of their personal data'. All sectors agreed the highest level was Extremely aware (Second Level Schools N=77,Further Education and Training 49, N=66) and second highest as Very aware (Second Level Schools N=58,Further Education and Training N=34, Higher Education N=57). When the relationship was tested there was a moderate level of significance with r=.529. Respondents from the three sectors provided generally similar responses to the item, 'To object to the use of their personal data'. All sectors identified the highest level as Extremely aware (Second Level Schools N=74,Further Education and Training N=45 and Higher Education N=58) and second highest as Very aware (Second Level Schools N=58,Further Education and Training N=24 and Higher Education N=50). The level of relationship had a low significance at r=.210. The sector responses to the item, 'To have the personal data corrected', had a high relationship with sectors agreeing with the three highest scale points first Extremely aware, second Very Aware and third Moderately aware. The level of the relationship when tested was strong positive significance at r=.763. While there was some similarity in responses from sectors to item, 'To have personal data deleted', it was relatively low. There was agreement on the highest level Extremely aware (Second Level Schools N=57, Further Education and Training N=45 and Higher Education N=57) however, there were differences in the other scale items. The level of significance was very low at r=.082. There was a moderate similarity between sector responses to item, 'To restrict the use of their personal data', with agreement of the highest level Extremely aware (Second Level Schools N=63,Further Education and Training N=47 and Higher Education N=60). The level of relationship was low significance at r=.216.

Cluster 3, Data breach

This cluster sought to gain respondents level of awareness about data breaches[18]. The cluster contained five items which included reporting to the organisations Data Protection Officer (DPO), assessing the breach, measures to stop the breach, advising about the breach and reporting to the Data Protection Commission (DPC). This cluster received N=499 responses

[18] Guidelines relating to data breaches can be found at https://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide

and 2 skipped (Non-responses). The focus was on data breaches. For the item, 'Inform the organisation's Data Protection Officer', 35% of respondents were Extremely aware and 28% were Very aware whereas 7% were Not at all aware and 9% were Slightly aware. The weighted average score for the item was 3.7 (Very aware). The item, 'Assess the scope and nature of the data breach', received 28% Extremely aware and 27% Very aware compared to 7% Not at all aware and 10% Slightly aware. The weighted average score for the items was 3.58 (Very aware). Respondents indicated 32% Extremely aware and 31% Very aware to the item, 'Put measures in place to stop the breach from reoccurring', and 6% Not at all aware and 10% Slightly aware. The weighted average for this item was 3.75 (Very aware). Regarding the item, 'Advise the relevant parties of the breach', 34% of respondents stated they were Extremely aware and 28% were Very aware, this is compared to 5% Not at all aware and 10% Slightly aware. The weighted average for the item was 3.76 (Very aware). Respondents indicated 30% Extremely aware and 23% Very aware to the item, 'Report the breach to the Data Protection Commission', compared to 10% Not at all aware and 12% Slightly aware. The weighted average score for the items was 3.52 (see Table 5). In general, there was a good level of awareness relating to data breach items.

Are you aware that the following steps should be carried out where a data breach occurs	
Item	*Weighted average*
Inform the organisation's Data Protection Officer	3.77
Access the scope and nature of the data breach	3.58
Put measures in place to stop the breach from reoccurring	3.75
Advise the relevant parties of the breach	3.76
Report the breach to the Data Protection Commissioner	3.52

Table 5 Cluster: Data breach, weighted average

Regarding sector responses to the item, 'Inform the organisation's Data Protection Officer', there was some similarity in responses. There was agreement in all sectors that Extremely aware was the highest preference (Second Level Schools N= 61,Further Education and Training N=47, Higher Education N=66). The level of relationship was very low with r=.084.With reference to item, 'Assess the scope and nature of the data breach' and the sectors there was some level of similarity in responses. The highest level was Moderately aware (Second Level Schools N=54, Further Education and Training N=25 and Higher Education N=56). When tested for similarity there was a moderate level of significance at r=.317. There was some similarity between sectors and the item, 'Put measures in place to stop the breach from reoccurring'. Both Second level and Higher Education identified Very aware as the highest level (Second Level Schools N=61, Higher Education N=61) whereas Further Education and Training selected Extremely aware (Further Education and Training N=35). The relationship between the two items was low at r=.158. There were some similarities between responses received from Sectors to the item, 'Advise the relevant parties of the breach'. All sectors identified the Extremely aware option as the highest and Very aware as the second highest. When tested for relationship there was a low level of significance at r=.186. There was some similarity between the sectors and the item, 'Report the breach to the Data Protection Commissioner'. All sectors identified the option Extremely aware as the highest (Second Level Schools N=49, Further Education and Training N=41 and Higher Education N=57). When tested for level of relationship there was very low significance r.081.

Cluster 4, Consent

This cluster explored the level of awareness relating to the criteria around consent[19]. The cluster contained four items relating to consent such as, freely given, request must be clear, can be

[19] Useful information on consent and the right to be informed is available on the Podcast https://www.dataprotection.ie/en/dpc-guidance/podcasts/know-your-data-episode-one

withdrawn and age for parental consent. This cluster received N=502 responses. Respondents indicated Extremely aware 39% and Very aware 32% to the item, 'Freely given by the individual' this is compared to 4% Not at all aware and 5% Slightly aware. The weighted average score for the item was 3.97 (Very aware). For the item, 'Requested in clear and unambiguous language', 38% were Extremely aware and 31% Very aware compared to 5% Not at all aware and 6% Slightly aware. The weighted average score for the item was 3.9 (Very aware). Respondents indicated the following levels of awareness to item, 'Understood that consent can be withdrawn at a future date', Extremely aware 37%, Very aware 30% compared to 9% Not at all aware and 7 % Slightly aware. The weighted average score was 3.83 (Very aware). Regarding the item, 'Understood that parental consent is required for those under 13 years of age', respondents indicated 40% Extremely aware and 24% Very aware whereas 9% were Not at all aware and 7% were Slightly aware. The weighted average for this item was 3.79 (Very aware). In general, there was a good level of awareness for the data breach items.

Consent - Consent to process personal data must be obtained from the individual, are you aware it must be?	
Item	*Weighted average*
Freely given by the individual	3.97
Requested in clear and unambiguous language	3.9
Understood that consent can be withdrawn at a future date	3.83
Understood that parental consent is required for those under 13 years of age	3.79

Table 6 Cluster: Consent to process data, weighted average

Relating to item. 'Freely given by the individual', and sector responses there was some similarity with all sectors agreed that Extremely aware was the highest level (Second Level Schools N=72,Further Education and Training N=52 and Higher Education N=72). The level of relationship between sectors was significant but low at r=.117. There was some similarity between the sectors regarding the item, 'Requested in clear and unambiguous language'. There was an agreed preference within the sectors to place the option Extremely aware at highest level (Second Level Schools N=71, Further Education and Training N=51 and Higher Education N=68). When tested for level of relationship there as a moderate positive significance at r=.393. There was high similarity in responses between the sectors relating to the item, 'Understood that consent can be withdrawn at a future date'. When tested for relationship there was a strong positive level of significance with r=.853. There was a high degree of similarity between sectors responses to the item, 'Understood that parental consent is required for those under 13 years of age'. When tested for relationship there was a very strong positive level of significance at r=.945.

Information and training

This section explored whether respondents had participated in GDPR related training and what level of training would they require. The questions received N=502 responses. Respondents stated No (91%) had not participated in data protection training provided by TUI however, 71% stated Yes, they had participated in GDPR training provided by their employer. Asked if they were interested in participating in GDPR training 55.4% said Yes and 44.6% said No (see Table 7).

Training - A data processor should provide training to staff and relevant persons		
	Yes	No
Have you participated in data protection training provided by TUI?	8.17%	91.83%
Have you participated in data protection training provided by your employer?	71.31%	28.69%
Are you interested in participating in data protection training?	55.40%	44.60%

Table 7: Training

When the data were explored by sector for the item, Participating in GDPR training provided by your employer, there was high levels of Yes indicated in all sectors, second level School N=133, Further Education and Training N=89 and Higher Education N=131, see Table 8 below.

Sector - Please indicate which sector you work in * Have you participated in data protection training provided by your employer? Crosstabulation				
		Have you participated in data protection training provided by your employer?		
		Yes	No	Total
Sector - Please indicate which sector you work in	Other (please specify)	5	2	7
	Second Level Education	133	63	196
	Further Education & Training	89	23	112
	Higher Education	131	55	186
Total		358	143	501

Table 8: Responses by sector participated in training

When asked what level of training in GDPR was required respondents indicated, Basic training 15%, General training 33%, Advanced training 21%, and None 29% (see Table 9).

What level of training do you require?	
Answer Choices	Responses
None of the above	29.64%
Basic, introduction to GDPR and individual rights	15.32%
General, key principles of GDPR and data processors obligation	33.67%
Advanced, processing data access request and data breach	21.37%
Other (please specify)	0.00%

Table 9: Level of training

From the responses N=332 indicated they would participate in training, of which N=76 indicated a preference for Basic training, N=165 chose General training and N=91 picked Advanced training. It is worth noting that nearly 70% of respondents indicated they were interested in participating in some level of GDPR training. A significant number of respondents had already engaged in some form of GDPR training with their employer or the union. This willingness to engage in training needs to be supported by the provision of suitable training options. It may be worth exploring collaborative training options with some employers.

Remote working during Covid-19 restrictions

In order to reduce the spread of Covid-19 government restrictions were put in place to limit social contact and movement in the community and workplaces. Since March 2020 employers and employees were requested (where possible) to work remotely. During lockdown periods schools, colleges and Higher Education institutes closed onsite activities and moved to emergency remote online teaching. This section of the survey sought to ascertain respondents' experiences of GDPR-related matters while engaged in emergency remote online teaching. In relation to the move to emergency remote teaching respondents were asked if their employers provided them with an encrypted device, 54% said No. Relating to the provision of secure access to online software while remote working, respondents were asked if their employers provided two factor authentication, 58% stated No. Respondents were also asked if their employers provided GDPR information for remote work, 59% stated No (see Table 10). It would seem that a large number of respondents were not provided with information, devices, and secure access for processing personal data while remote working.

During the Covid-19 emergency restrictions many public servants were required to work remotely. If you have worked remotely, please respond to the GDPR-based statement below		
	Yes	No
My employer provided me with an encrypted device for remote work	45.88%	54.12%
My employer set-up two factor authentications for me to access data	41.77%	58.23%
My employer provided information on GDPR procedure for remote working	40.57%	59.43%

Table 10: Remote working

When the data for item, 'My employer provided me with an encrypted device for remote working', is explored per sector it can be observed that respondents in the Higher Education reported a higher number that did not received encrypted device (No N=110, Yes N=73). Respondents in the Further Education and Training sector reported a more balanced response (No N=54 and Yes N=58). Relating to the item, 'My employer set-up two factor authentication for me to access data', when responses are explored by sector it can be observed that both Second Level Education and Further Education and Training reported a significant number of No (Second Level Schools N=121, Further Education and Training N78). On the other hand, Higher Education respondents indicated a strong Yes (Yes N=97 and No N=82). In relation to the item, 'My employer providing information on GDPR procedure for remote working', all sectors indicated a negative response No, (Second Level Schools N=113, Further Education and Training N=66, Higher Education N=11). With regards to experiences of remote working and GDPR matters, a risk assessment cluster consisting of seven items was put to respondents. The cluster used a Likert scale comprising of five points, 'Very low risk, Low risk, Medium risk, High risk and Very high risk'. The Risk Level indicator for weighted average scores is presented in Table 11.

Risk level	Weighted score
Very low	less than 1
Low	1 or above but less than 2
Medium	2 or above but less than 3
High	3 or above but less than 4
Very high	4 to 5

Table 11: Risk level indicator

Respondents were requested to identify the level of risk they associated with GDPR items while they were working remotely. Regarding the item, 'Unauthorised use of electronic device provided by the employer', respondents identified Very high risk 8%, High risk 10% compared to Very low risk 27% and Low risk 32%. The weighted average score for this item was 2.4 (Medium risk). Respondents indicated the risk level to item, 'Breach of confidentiality of personal data', as Very high risk 10%, High risk 12% and Very low risk 9% and Low risk 34%. The weighted average score for the item was 2.6 (Medium risk). For the item, 'Unauthorised access to other individual's personal data records', respondents indicated; Very High risk 8%, High risk 10% compared to Very low risk 27% and Low risk 33%. The weighted average score was 2.38 (Medium risk). Respondents indicated the risk level for the item, 'Exposure to cybercrime', as 11% Vey high risk, 15% High risk and 11% Very low risk and 32% Low risk. The weighted average score for the item was 2.83 (Medium risk). In terms of the item, 'Hacking into devices and software programmes', the respondents indicated the following, very high risk 10%, High risk 15% compared to Very low risk 12% and Low risk 34%. The weighted average score for the item was 2.78 (Medium risk). For the item, 'Unauthorised use of your personal data', respondents identified the following risk levels, Very high 8%, High 12%, compared to Very low 15% and Low 38%. The weighted average score for the item was 2.59 (Medium risk). Respondents associated the risk level for the item, 'Privacy breaches', as 10% Very high, 13% High whereas 14% Very low and 15% Low. The weighted average scores for the item were 2.7 (Medium risk). The full cluster of items with risk levels, average scores for each item can be observed in Table 12.

From your experience of remote working please indicate the level of risk relating to the following GDPR matters	
Item	*Weighted average*
Unauthorised use of electronic device provided by the employer	2.4
Breach of confidentiality of personal data	2.6
Unauthorised access to other individual's personal data records	2.38
Exposure to cybercrime	2.83
Hacking into devices and software programmes	2.78
Unauthorised use of your personal data	2.59
Privacy breaches	2.7

Table 12 Cluster: Risk level during remote working

When responses are explored for item, 'Unauthorised use of electronic device provided by the employer, the risk level identified by sector vary. The highest indicators for the sectors were Second Level Education No Risk N=52, Further Education and Training Low risk N=41 and Higher Education Low Risk N=68. Second Level education indicated the highest Very high-risk level at N=23, see Figure 29. When the sectors were tested for similarity, there was a very weak association with r=.008. The risk levels per sector to item, 'Breach of confidentiality of personal data', received strong support for the indicator Low risk (Second Level Schools N=58,Further Education and Training N=39 and Higher Education N=74). The indicator Medium risk also received high level of support (Second Level Schools N=46 and Higher Education N=46), see Figure 30. When tested for level of significance the was a very weak result at r=.011. For the item, 'Unauthorised access to other individual's personal data records', the sectors indicted Low Risk as the highest level (Second Level Schools N=54,Further Education and Training N=37 and Higher Education N=71). In terms of Very high risk the sectors differed with Second Level Schools N=24,Further Education and Training N=5 and Higher Education N=12, see Figure 31. The level of significance between the sectors was weak with r=.086. The item, 'Hacking into devices and software programmes', the sectors indicated Low Risk (Second Level Schools N=59,Further Education and Training=36, Higher Education N=72) and Medium Risk (Second Level Schools N=42,Further Education and Training=36, Higher Education N=55). There was also strong support indicated for High risk (Second Level Schools N=32,Further Education and Training=18, Higher Education N=25), see Figure 32. When tested for association there was a very weak level of significance with r=.003. In terms of the item, 'Unauthorised use of your personal data', respondents in the sectors indicated high levels of support for the indicator Low risk (Second Level Schools N=59,Further Education and Training N=42 and Higher Education N=84). Also, there was support for the indicator Medium risk (Second Level Schools N=46,Further Education and Training N=33 and Higher Education N=44), see Figure 33. The level of significance was very weak at r=.006. The item, 'Privacy breaches', received high sectorial support for risk levels, Low risk (Second Level Schools N=54,Further Education and Training N=40 and Higher Education N=75) and Medium risk (Second Level Schools N=45,Further Education and Training N=36 and Higher Education N=50). Second level also indicated high support for risk level Very high-risk N=30. When tested for significance it was very weak at r=.001. For the item, 'Exposure to cybercrime', there was strong support for the indicator Low risk (Second Level Schools N=54,Further Education and Training N=33 and Higher Education N=70) and Medium risk (Second Level Schools N=51,Further Education and Training N=36 and Higher Education N=55), see Figure 35. When tested for significance level it was very weak at r=.011.

Respondents were also asked if they had experienced GDPR breaches while they were working remotely. Of the respondents 81% stated they did not experience any GDPR breaches during remote working. Breaches that were experienced (by 19% of respondents) included Data Breach 4.7%, Unauthorised access 1,7%, Deletion of data 3.9%, Loss of device 2.3%, Privacy breach 3.4%, and Hacking 2.1%, see Table 13. The Other option received 6.5% with some text

contributions, these included matters such as, circulation of private email addresses, document emailed to the wrong person, documents used without consent, unauthorised recording of online classes, equipment break-down, unauthorised access to online platforms, sharing documents without encryption or password protection and use of inappropriate language and images while online.

During remote working have you experienced any of the following	
Answer Choices	Responses
Data breach (unintentional release of private data to third parties)	4.77%
Unauthorized access (a person/programme gaining access to your account/files)	1.74%
Deletion of data (accidental deletion of personal data/files)	3.90%
Loss of device (accidental loss or theft of a storage device, USB stick, phone, laptop, tablet)	2.39%
Privacy breach (a person/programme using your personal data without your consent)	3.47%
Hacking (person/programme gaining unauthorized access to your device for malicious reasons)	2.17%
None	81.56%
Other (please specify)	6.51%

Table 13: GDPR issues experienced while remote working

Survey textbox contributions

The survey also provided some Text Box options for respondents to provide additional information, suggestions, and opinions. The text provided by the respondents was grouped into general areas and drafted into a narrative. Many of the respondents surveyed suggested that there was a need for greater awareness of current data protection policy and procedures. One respondent said that there was a need for '*practical advice on how to store important files on OneDrive and manage passwords'*. The respondents recommended that training relating to data protection policy, procedure and risk assessment be given to union representatives and staff by both the union and employers. It was noted by some respondents that this training be specific to the employment role and updated on a yearly basis. Some respondents suggested that the language used to explain GDPR should be written in plain English to make it more accessible. One respondent noted, '*In cases where individuals whose command of English is very limited, any necessary signing of GDPR agreements has to be in very plain English, or in their mother tongue, otherwise they have very little understanding of what they are signing, or why'.*

Regarding remote teaching the respondents in the survey suggested that this area be given clarification about GDPR issues. It was noted by one participant that the use of organisational VPN was one method to protect data. One respondent said, '*I think that we should have access to files on an online portal that would give us greater security with regards to work files'. Some* respondents noted that they were using their own personal computer equipment and that there were issues with home printers and screen size. Access to shredders, especially during exam marking, was of particular concern. Another concern was the inequity of computers and Wi-Fi service which were unfit for work purposes. Although some institutions did give respondents computers, others are waiting for suitable equipment from their institution. The members argued that the equipment provided to date is unsuitable for their practice and that they had to use their own personal equipment placing strain on family resources. In addition, a respondent stated, ' *I would have concerns for those working on older personal laptops, that their laptops may not be suitable, they should be offered compliant equipment for use to be GDPR compliant. I would suggest that college IT department should offer to assess anyone's personal equipment'.* A respondent noted, '*To avoid GDPR issues I do not print or keep data on my PC's memory, I keep it on work supported websites'.* It was suggested by the survey respondents that greater security could be achieved using online portals to access work files and storing information on work supported sites. A respondent noted, '*Very difficult to maintain privacy of data particularly when marking exams at home'.* While others argued that better

understanding was needed in areas around encryption information and '*and the risk with unprotected email on smartphones'*. A participant noted that data privacy provided benefits of data processing, however another stressed that there was little privacy regarding video class recordings. Respondents raised issues about employers using personal data without attaining informed consent. One respondent stated, '*At the start of the pandemic, two people in my household were sharing a laptop, because that is all we had. I think my employer should do a lot more to allow me to be compliant from a GDPR'.* Overall respondents surveyed did not experience data protection breaches. Some data breaches were noted relating to email communication and the including of email addresses in the CC function. It was also suggested by a respondent that institutional breaches occurred by using private data in a CV for other than the original purposes. Other breaches involved email data being changed and used, recording of lectures, as well as online lecture notes being accessed and changed without the lecturer's knowledge or consent. A respondent suggested that the way data is transferred was an area that required attention. For another respondent, a particular concern relating to online access was that *'People falsely posing as students attend web classes and caused disruption. Abusive comments of a sexual and homophobic nature'.* Several breaches of data protection were reported by respondents surveyed such as emails shared to wrong recipient. In the Question 12 comment textbox respondents disclosed several types of data protection breaches that they were aware of, these included the following:

- The disclosure of individuals names and email address (in CC list) in workplace communications by emails and WhatsApp groups.
- Information addressed and sent to the wrong individual.
- Employer using CV information for purposes other than a selection process.
- Unauthorised access to virtual meetings.
- Unauthorised recording of online teaching.
- Issue to do with the secure sharing of information.
- The circulation documents that are not password protected.
- The use of own personal equipment for work purposes.

It was suggested by a respondent that the union could facilitate training in relevant GDPR areas if required. Respondents suggested that training was needed, this training should be specific to the sector and the role (teacher, lecturer, researcher etc.,). The training should be provided in short sessions at times that are appropriate to members. It was also noted that the employer should also be involved in some of the training. One respondent suggested, '*…the union looks at how Institute management /is handling GDPR, and developing agreements, for example, the process around assessing whether an issue falls under GDPR, before invoking suspected GDPR breach process'.* Some respondents suggested that short information leaflets could be of assistances (one pager) with other respondents suggesting training was also needed relating to software used for work, security measures and cybercrime. A respondent noted, '*Clarification about GDPR would be beneficial in terms of remote teaching'*.

Since March 2020 due to Covid-19 pandemic restrictions most teachers and lecturers have had to move to emergency remote teaching for specific periods. This move to remote work has increased the potential risk level of GDPR issues arising. Respondents argued that there was a need to provide GDPR training to Workplace Reps and Branch Officers, and that the training be relevant and accessible. In addition, it was suggested that there was a need for sector-specific information sheets and check lists that could assist members in their workplaces.

Conclusion

The introduction into law of GDPR has strengthened the rights of individuals to have their personal data protected and their privacy respected. The legislation requires data controllers

and data processor to raise standards related to the use of personal data and to have procedures and policies to demonstrate compliance with the terms of the legislation. In circumstances where non-compliance can be proven, the law provides authority for the Data Protection Commission to impose sanctions, including financial sanctions in the form of fines. The legislation also requires data processor and data controllers to promote awareness of GDPR, including the provision of information to data subjects and training for staff. This research sought to ascertain GDPR awareness levels of teachers and lecturer employed in the tertiary education sectors. And to explore possible GDPR risks that may arise during emergency remote working due to Covd-19 restrictions. It is clear from the results that respondents in all three sectors (Second level Schools, Further Education and Training and Higher Education) have a high general level of awareness of GDPR including the key principles and individual rights. In terms of data breach procedures and consent, respondents indicated a medium level of awareness. Respondents indicated they were aware of the importance of GDPR and the need to adhere to the legal requirements. Respondents also indicated that they had participated in some form of GDPR training provided by their employer or the union and were willing to participate in more GDPR training. Respondents sought easily accessible GDPR information, fact sheets, leaflets, social media and visual product information. Furthermore, respondents were aware of potential risks associated with GDPR when remote working due to the Covid-19 emergency restrictions. Respondents identified potential risks that could lead to GDPR breachers will remote working and in some cases disclosed that they have experienced breaches relating to loss of data, unauthorised access, unauthorised use and sharing of data. Respondents also raised concerns about the lack of provision of appropriate equipment and software for remote working. Respondents suggested that GDPR training and information events could be jointly provided by the employers and union working together. GDPR requirements were common to all sectors and there was a need to have a coordinated approach to training and promoting good practice. This could be assisted with the development of a common Continue Professional Development GDPR module for the education sectors. Investment in GDPR awareness and training could assist in reducing the risk of potential data breaches, this would have a long-term benefit in terms of reduced exposure to possible investigations and sanctions. The data shows that teachers and lecturers as professional are willing to engage in GDPR training, measures should be considered on how best to engage with staff and provide the necessary training options.

References

Companies Registrations Officer https://www.cro.ie/eN=ie/Society-Union/RFS-Trade-Unions

Creswell J., Creswell J. (2017) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, Sage.

Data Protection Commission https://www.dataprotection.ie/

European Commission (2018) *Fact Sheet- How will data protection reform help fight international crime*, available at URL link http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41527 .

Kincheloe J., McLaren P. (1994, pp138-157) *Rethinking Critical Theory and Qualitative Research*, in Denzin N. and Lincoln Y. (1994) Handbook of Qualitative Research, Sage International.

Lambert P. (2016) *Data Protection Law in Ireland: Sources and Issues*, 2nd Edition, Clarus Press, Ireland.

Miles M., Huberman M. and Saldana R. (2019) *Qualitative Data Analysis: A Methods Sourcebook*, Sage, USA.

Robson C., McCartan K., (*2016) Real World Research, A resources for social scientists and practitioner-researchers,* Wiley.
Statistical software package used, IBM SPSS Statistics, version 27, see website https://www.ibm.com/search?lang=en&cc=us&featureFlags=v1-1&q=SPSS
Survey Monkey GDPR Statement https://www.surveymonkey.com/curiosity/surveymonkey-committed-to-gdpr-compliance/
Thomas G., Pring R. (2004) *Evidence-Based Practice in Education*, Open University Press.
Walley P. and Kimber C. (2016) *Cyber Law and Employment*, Round Hall.

[i] The author served two five-year secondments with the TUI in the role as Assistant General Secretary including Data protection Officer, he returned to his Lecturer position in the Dublin Institute of Technology now the Technological University Dublin in September 2021.
Paper citation: Kenny A. (2021) *Data Protection Awareness Survey of Tertiary Sector Teachers and Lecturers in Ireland,* TUI, Ireland.