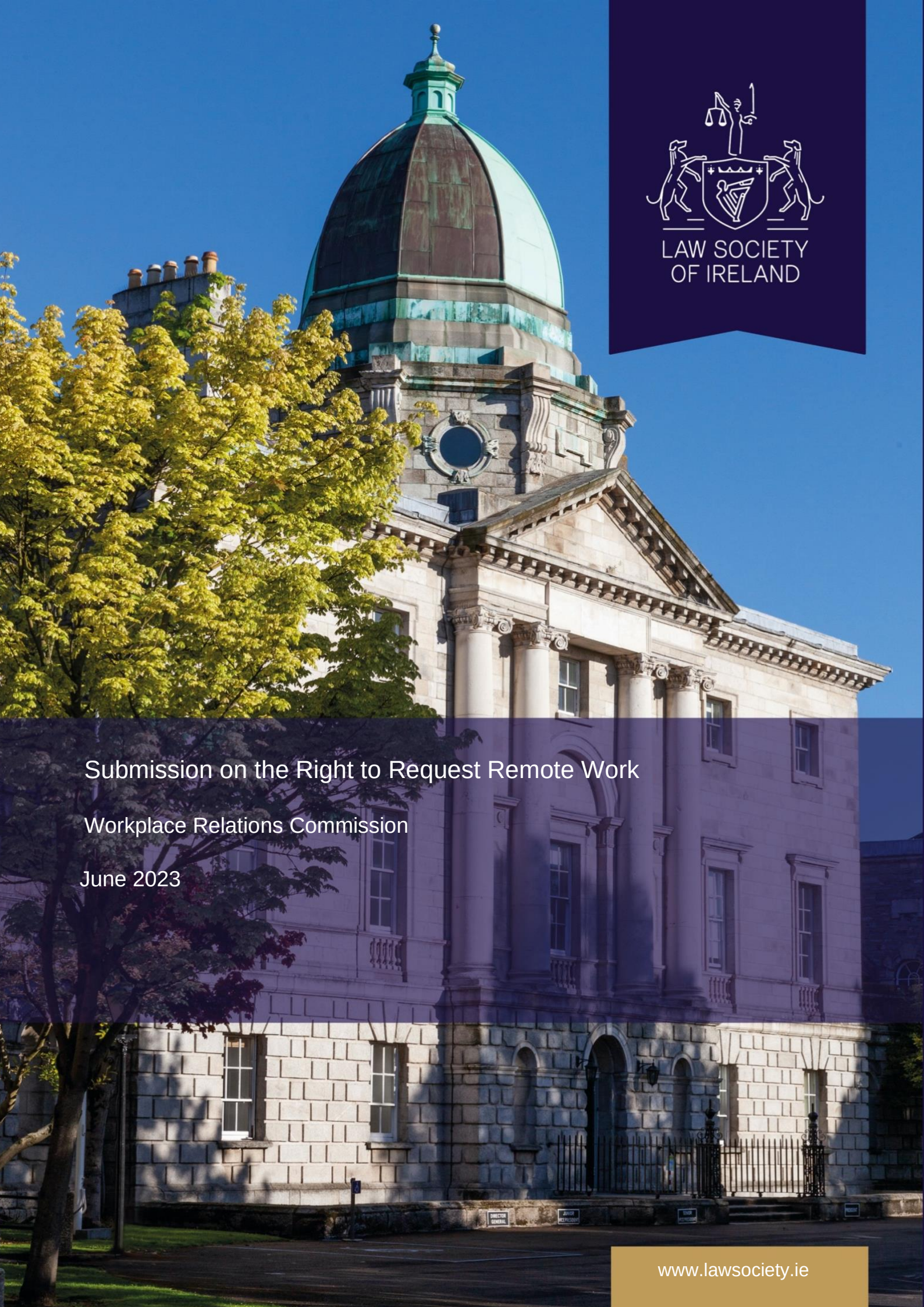

LAW SOCIETY OF IRELAND

Submission on the Right to Request Remote Work

Workplace Relations Commission

June 2023

www.lawsociety.ie

1. Introduction

1.1 The Law Society of Ireland (the "**Society**") welcomes the opportunity to participate in this Workplace Relations Commission (**WRC**) consultation on the development of a Code of Practice on the Right to Request Remote Working (**COP**) as required by the *Work Life Balance and Miscellaneous Provisions Act 2023* (the "**2023 Act**").

1.2 In this submission, our Employment & Equality Law Committee (the "**Committee**") sets out its observations and recommendations in respect of remote working arrangements based on practitioners' experience in advising employers and employees, particularly since the pandemic.

1.3 The Committee is of the view that the guidance provided in the COP should be practical, not overly prescriptive (wherever appropriate), and should be prepared with regard to the fact that the vast majority of employers in Ireland are SMEs with almost one third of employers having less than 10 employees (2020 CSO figures).

1.4 This submission should be read in conjunction with our preliminary observations on the need for further guidance on remote working as detailed in an August 2020 submission to the Department of Business, Enterprise and Innovation.

Law Society Recommendations

- The COP will set out practical guidance for employers and employees on the steps to be taken to ensure compliance with the 2023 Act.

- It should provide clear guidance to ensure compliance with existing employment law and other relevant statutory obligations which include health, safety and data protection and the Organisation of Working Time Act (**OTWA**).

- Issues of where responsibility lies with regard to the costs associated with remote offices and location must be addressed to enable employers to provide clear policy and procedure documents.

- Specifically, the Committee makes the following recommendations which arise from the collective, practical experiences of its members:

  Recommendation 1: *(see section 2 of this submission)* The COP should clarify that the remote working arrangement must be within the Republic of Ireland and an employee's ability to work in a location other than the employer's place of work, cannot be extended beyond Ireland.

  Recommendation 2: (*section 2)* The COP should address an employer's right to require an employee to attend at the employer's place of business for training days, employee wellbeing or other similar initiatives.

  Recommendation 3: (*section 3)* The COP should outline the core factors for an employee to include when self-assessing the suitability of their proposed working location and submitting their application. The Health & Safety Authority's (**HSA**) *Occupational Safety and Health Guidance on Remote Working Checklist* is a helpful resource, focusing on practical aspects of the working environment e.g. lighting, heating, ventilation and physical infrastructure. It also addresses the ergonomic set up of a workstation, communication, wellbeing and incident reporting. As the checklist is

extensive, it may be challenging for employees to complete. As such, attaching a simple questionnaire to the COP (based on the HSA's checklist) would be helpful.

Recommendation 4: *(section 3)* Additional information should be included in the COP to ensure that employees also address a range of issues such as data protection/confidentiality, cyber security and working time records. Further information about why this should be included is set out below.

Recommendation 5: *(section 3)* The extent of an employee's responsibility to self-assess the suitability of the location should be clarified.

Recommendation 6*: (section 3)* To streamline the remote working application process, information that employers receive in order to be in a position to assess the suitability of a remote working location should be prescriptive (e.g. the questionnaire/template suggested above). This will ensure fairness in remote working assessments with every employee measured on the same information as regards the suitability of the workplace location. It is recommended that this questionnaire cannot be used by an employer to delay the processing of an application, or in substitution for meeting the employer's legal obligations under the 2023 Act.

Recommendation 7: *(section 4)* The requirements of the COP will align with the information an employee is required to include in their initial application. It is the Committee's view that the COP should provide guidance on non-exhaustive considerations which an employer may have regard to in considering requests for remote working. This is particularly relevant should the employer refuse an application, given that they must provide reasons for the refusal.

(***Note***: In the UK, legislation sets out the specific business grounds for refusal to accept an employee's request for remote working. It is the Committee's view that this goes further than what is set out in section 21, creating ambiguity for both employers and employees. The specific business reasons available in the UK include the burden of additional costs, detrimental effect on ability to meet customer demand, inability to re-organise work among existing staff, inability to recruit additional staff, detrimental impact on quality, detrimental impact on performance, insufficiency of work during the periods the employee proposes to work, planned structural changes.)

Recommendation 8: *(section 4)* The COP should offer clear examples of where an employer can extend their response timeframe (e.g. to take health and safety advice in relation to a proposed remote working arrangement). As it stands, this section could enable an employer to unjustifiably delay responding to an employee's request.

Recommendation 9: (*section 5)* The COP should offer guidance on how employers can assess whether a remote working arrangement is having a '*substantial adverse effect*' on the operation of their business, profession or occupation, and encourage ordinary employer/employee communications prior to the issue of any summary notice of intention to terminate an arrangement.

Recommendation 10: *(section 6)* The 2023 Act does not make explicit reference to health and safety measures when considering the request to work from home. The COP should direct employers and employees to their obligations under the relevant legislation and the HSA guidance.

Recommendation 11: *(section 6)* The COP should refer to the HSA guidance for details of the key physical infrastructure and technical specifications required for an adequate, safe and healthy home working environment e.g. risk assessments in employees' homes and providing office furniture (e.g. desks, monitors and chairs).

Recommendation 12: (section 6) The COP should confirm that a risk assessment can be completed virtually or in person. Guidance as to the frequency with which risk assessments should be reviewed and updated should be clear (e.g. every two years).

Recommendation 13: (*section 6)* The Committee previously identified a number of health and safety related matters in its submission on the Draft Scheme of the Work Life Balance and Miscellaneous Provisions Bill 2022, some of which have been addressed in the legislation. It would be helpful if the following remaining issues could be addressed in the COP:

(a) How employers should deal with home work-related accidents while employees are working from home, in particular any potential need for employers to make employees aware of procedures for reporting work-related accidents, ill health or any other health and safety concern whilst working from home.

(b) If the employee's home becomes a workplace, employers should be encouraged to ensure that they have appropriate cover in place (to include remote working and use of the employer's equipment in their employees' homes).

Recommendation 14: (*section 7)* The COP should clarify that, although an employee may be permitted to work remotely, the obligations under the OWTA remain. Employees' obligations to comply with the systems put in place by the employer to record time should be referenced in the COP so that their responsibilities are equally clear.

Many employers who had workplace-based clocking in/out systems to record the working hours and breaks of their employees, are now faced with the challenge of recording information for a remote or hybrid workforce. Employees should be required to acknowledge these requirements when making a remote work application, to declare their willingness to work in a manner which is compliant with the OWTA and to engage and operate such time management tools as the employer may specify. Consideration should be given to the extent of employee responsibility for managing these matters and a self-declaration form (to be completed by the employee) which could be incorporated into a request for remote working may be useful in confirming an employee's willingness to:

1. Work the days/hours and take the necessary breaks required under their contract of employment and the OWTA;

2. Record their working hours, breaks and holidays in accordance with whatever time management tool their employer provides to them in a timely and accurate manner, submitting records to the employer as required under that system;

3. Notify their manager of any missed breaks or longer working hours; and

4. Participate in any necessary training on relevant systems.

Recommendation 15: *(section 8)* Guidance on best practice around how to manage remote working employees and the extent of obligations to monitor this would be welcome. Co-operation by employees in the ongoing assessment of working hours, breaks and work life balance is also required. Recent HSA guidance on managing psychological hazards in the workplace specifically identifies that lone and remote working can contribute to psychosocial risk. As such, it recommends that employers conduct a risk assessment to identify any such risks and put supports, policies and training in place to deal with such issues. Employee co-operation and participation in the implementation of such steps is necessary.

Recommendation 16: (*section 8)* Ensure that Right to Disconnect policies are updated to reflect remote working arrangements and, in particular, ensure that such policies include a recommendation for employees to operate during their core hours only and not to respond to emails or messages outside of those times. Employers who operate across different time zones should ensure that employees are reminded to only be available for work during their normal working day.

Recommendation 17: (*section 8)* An employee declaration (to accompany a remote work request) that they will comply with measures implemented to enable them to disconnect while working remotely would be welcome.

Recommendation 18: (*section 9)* Various DPC guidance documents consider the following relevant issues which should be addressed in data protection considerations for the COP (highlighted in bold throughout):

(a) Network access

The DPC's Data Security Guidance addresses network access concerns.

As remote access can leave a server open to attack, **specific guidance** should be provided to employers on what **technical security measures**, **security assessments, contractual arrangements and agreed standards of management** are required to appropriately manage the risks associated with remote access to the network. Specifically, guidance on **trusted networks or cloud services and multifactor authentication for remote access** is needed for businesses which are engaged in remote working without dedicated IT departments.

The DPC's guidance on Protecting Personal Data When Working Remotely states that, where possible, an employee/worker should only use their organisation's trusted networks or cloud services. If the employee is working without cloud or network access, they should ensure that any locally stored data is adequately backed-up in a secure manner. **Remote workers should comply with any organisational rules and procedures** about cloud or network access, login and data sharing.

The Data Protection in the Workplace guidance recognises that monitoring software (e.g. keystroke logging or "tattle ware") is extremely intrusive and any attempt to use it must be objectively and demonstrably justified and proportionate. It should be borne in mind that the use of recording mechanisms to obtain data (which includes monitoring an employee's activity when working from home) without an individual's knowledge is generally unlawful. **All employees should be given a policy on email and internet use** in the workplace (i.e. an acceptable usage policy) which clearly sets out an employer's policy on computer and internet usage, including the use of social media on an employer-owned PC or laptop.

For employees, guidance is needed on the **rules and procedures** around cloud or network access, login procedures, appropriate use of wireless networks, secure web sessions and data sharing when accessing the employer's network.

In addition, **specific issues an employee should** consider and address when making a (section 20) request to work remotely include:

- Does their organisation provide secure network access/VPN access to the organisation's systems and can they access those from the remote work location?

- If there is no access to the organisation's network, is their personal internet secure (e.g. is open Wi-Fi shared with others in that location) and can they keep work information separate from other data on that network?

- Can the employee confirm that they can comply with the organisation's acceptable usage policy, any other relevant IT policies and security requirements in any applicable organisation policy when working remotely?

(b) The use of portable devices

The Data Security Guidance states that use of portable devices when working remotely poses a number of concerns from a data protection perspective. The Remote Working Guidance adds the **following requirements in respect of the use of** employees/other workers' **portable devices when working remotely**:

- Take extra care that devices, such as USBs, phones, laptops, or tablets, are not lost or misplaced.
- Ensure their computer, laptop, or device is used in a safe location e.g. where they can keep sight of it and minimise who else can view the screen, particularly if working with sensitive personal data.
- Lock their device if they have to leave it unattended for any reason.
- Make sure devices are turned off, locked, or stored carefully when not in use.
- Use effective access controls (such as multi-factor authentication and strong passwords) and, where available, encryption to restrict device access, and reduce risk if a device is stolen or misplaced.
- When a device is lost or stolen, take immediate steps to ensure a remote memory wipe, wherever possible.

Updated **guidance on acceptable encryption/pseudonymisation standards** and guidance on the storage of decryption keys should be provided to all employers and employees engaged in remote working. Additionally, an employee's section 20 request should consider and address:

- Whether they will be working in a location where work devices can be accessed by other people; and
- What security measures can/must they take to protect the device, e.g. not to use devices in common areas and to lock it away after work hours.

(c) IT security & updates

The Data Security Guidance highlights the importance of appropriate anti-virus software, firewalls and patch management systems to protect portable devices and networks from infection and malware. The Remote Working Guidance further states that a remote worker should make sure that devices have the necessary updates, e.g. to operating systems (iOS or android) and antivirus software.

Additional guidance should be provided detailing the recommended **technical specifications of anti-virus software** and clarifying the responsibility of employees and employers to maintain and ensure protective measures are kept up to date when working remotely. Further detail on the DPC's recommendation to **retain records of the employee's patch installations on an employer's system should be provided**. The guidance should also clarify whether **incident response plans** may need to be updated to report data security incidents which arise in the context of remote working.

(d) Physical security

As set out in the Data Security Guidance, in addition to the technical security measures, data controllers should consider what **physical security measures** are necessary to ensure the security and integrity of any personal data they process.

The Remote Working Guidance considers the physical security settings of devices and protecting personal data stored in hard copy/manual form, such as paper records. When someone is **working remotely with paper records**, they must take steps to ensure the security and confidentiality of these papers e.g. keeping them locked in a filing cabinet or drawer when not in use, disposing of them securely/shredding when no longer needed and making sure they are not left somewhere they could be misplaced or stolen. If someone working remotely is dealing with records which contain special categories of personal data (e.g. information about health, trade union membership or information that identifies another person's sex life (including marital status, details of pregnancy, maternity leave etc.), they should take extra care to ensure security and confidentiality and **only remove such records from a secure location where it is strictly necessary to carry out the work**.

Where possible, an employee should keep a **written record of all papers and files which have been taken home** in order to maintain good data access and governance practices.

Further guidance on the appropriate physical security measures to adopt when remote working should be provided to employers and employees. For example, the guidance should outline the importance of **ensuring confidentiality in the remote working space** (particularly where it is a shared living space or working hub), the importance of **securely locating the employee's remote working devices so that screens cannot be viewed by other household members or hub users, and ensuring devices are locked/switched off when not in use** should be addressed. Guidance should also outline the proper procedure for storage and disposal of hardcopy files containing personal data.

Recommendation 19 (*section 9)* As compliance by employers with data protection obligations is dependent on the actions of employees in a remote work environment which is controlled by the employee, we recommend that a request for remote work would address the suitability and security of the work area.

Recommendation 20: (*section 9)* The obligation to ensure a proper and safe place of work, ensuring data security, confidentiality, and the protection of intellectual property at a place of work are paramount considerations for employers. As such, employees should acknowledge these requirements when making a remote work application and declare their willingness to engage and implement any appropriate requirements to ensure data security. Perhaps an undertaking from an employee to comply with appropriate DPC guidance on remote working and to properly utilise any tools and policies provided by the employer could be incorporated into a request for remote

working. Employee compliance is essential if the employer is to meet its ongoing obligations under GDPR and the Data Protection Act 2018.

Recommendation 21: (*section 9)* We recommend that the WRC engages with the DPC on the above cumulative guidance prior to publishing the COP to produce a single point of reference (either in the COP or as an appendix to it). This could set out short, practical guidance for employers and employees on data protection and security which is specific to remote working arrangements. For example, the one-page Remote Working Guidance document (March 2020) contains simple and practical information for employers and employees about devices, emails, remote access and paper records.

Recommendation 22: (*section 9)* Employers should consider whether they need to conduct a Data Protection Impact Assessment or other risk assessment (specifically for high-risk roles, such as a Director of HR with access to employee medical data) as part of the implementation of their overall remote working arrangements or when considering requests made by employees who will be handling personal data or sensitive categories of data while working outside the employer's place of business.

Recommendation 23: (*section 9)* Guidance is required on the standard of the workspace from a data protection perspective. For example, employees in shared living accommodation may not be able to illustrate that their remote work location is appropriate to ensure adequate confidentiality and adherence to data protection rules for business-sensitive work. It is acknowledged that there will be cohorts of employees who will find it more difficult than others to identify a suitable work area in their homes. The obligation to ensure a proper and safe place of work, ensuring data security, confidentiality, and the protection of intellectual property at a place of work are paramount considerations for employers. Employers must be permitted to refuse requests for remote working where there are concerns relating to these issues, whether the work is being done in shared accommodation or in remote working hubs where several people are working side-by-side.

Recommendation 24: *(section 10)* The COP should define who is responsible for the cost of any modifications needed to set up a remote workstation.

Recommendation 25: *(section 10)* The cost of such modifications and/or minimum infrastructure should not create an additional significant administrative and financial burden for employers or employees.

Recommendation 26: *(section 10)* The COP should clarify who bears the financial burden of providing equipment to the remote working environment and place clear limits on what each party is responsible for.

Recommendation 27: *(section 11)* While many of these recommendations will be directly relevant to flexible working, we would recommend that a further consultation be undertaken in relation to Part II.

2. Preliminary observations

2.1 Threshold for COP to apply

The 2023 Act defines a "*remote working arrangement"* as:

"an arrangement whereby some or all of the work ordinarily carried out by an employee...is provided at a location other than at the employer's place of business without change to the employee's ordinary working hours or duties."

The reference to "some" in the definition will mean that all remote working arrangements (irrespective of frequency or duration) will be protected by the provisions of the 2023 Act.

As such, consideration should be given to the impact on employers of having to manage *ad hoc* remote working arrangements of temporary and short duration as well as more fixed and permanent arrangements.

3. Requesting a Remote Working Arrangement (Section 20)

3.1 An employee's request to work remotely must include the following information:

(i) Provide eight weeks' notice in writing and be signed by the employee;

(ii) Specify the details of the remote working arrangement, proposed start date and, where applicable, end date; and

(iii) Specify, having regard to the COP:

(A) The employee's needs;

(B) Details of the proposed remote working location; and

(C) Information as may be specified in the COP on the suitability of the proposed remote working location.

4. Employers Obligation to Consider a Remote Working Request (Section 21)

4.1 An employer must consider an employee's remote working request, having regard to:

a. The employer's needs;

b. The employee's needs; and

c. The requirements of the COP.

5. Terminating the Remote Working arrangement (Section 22)

5.1 Section 22 prescribes the circumstances in which an employer can terminate a remote working arrangement where it is having a '*substantial adverse effect on the operation of his or her business, profession or occupation'* by reference to specific factors listed in section 2(1)(a) to (d).

5.2 An employer, in making this decision, is required to consider (i) his or her needs, (ii) the employee's needs, and (iii) '*the requirements of the code of practice'*.

6. Miscellaneous legislative considerations

6.1 Below, the Committee provides its views on the interaction between the 2023 Act and other employment-related legislation.

6.2 Under the Safety, Health and Welfare at Work Act 2005 (as amended) (the "**2005 Act**"), all employers are required to take steps to ensure that their employees are working in as safe an environment as is reasonably practicable. It is vital that employers familiarise themselves with their ongoing health and safety obligations, which apply regardless of whether employees are working in the office or remotely. This means that employers must conduct risk assessments of their employees' working environments and review them regularly to ensure that employees working from home remain safe and healthy.

6.3 Section 8 of the 2005 Act establishes the general duties of an employer in terms of the health and safety standards which they are expected to adhere to. An employer must do what is "reasonably practicable" to ensure the safety, health and welfare at work of its employees. There is no express leniency or flexibility in terms of the performance of these duties as they apply to the home working environment which is impractical where, for example, an employer has (justifiably) no right to inspect the home working environment.

6.4 In the UK, employers have similar health and safety obligations and are responsible for managing health and safety risks in their businesses. For example, similar to the HSA, the Health & Safety Executive provides guidance for employers on managing risks and risk assessment at work. Details such as risk assessment templates and common workplace risks are provided. Similarly, ACAS (Advisory, Conciliation and Arbitration Service) provides guidance to employers on conducting a '*suitable and sufficient*' risk assessment of employees' working environments. ACAS also advises that *"if an employer is not able to carry out a full risk assessment, they should provide their employees with information on working safely at home".*

7. Organisation of Working Time Act Obligations (OWTA)

7.1 Employers have a statutory obligation to maintain working time records for each employee on a daily basis, including start and finish times, rest breaks, daily breaks and weekly breaks, which can be recorded electronically or in manual form under the OWTA. They must also ensure that employees avail of their entitlements under the OWTA.

8. Right to Disconnect/Employee Wellbeing

8.1 The WRC's *Code of Practice on the Right to Disconnect* reminds employers of their obligations and aims to ensure that workers understand their rights around refraining from engaging in work-related electronic communications (e.g. emails, phone calls or other messages) outside normal working hours.

8.2 Three rights are enshrined in the Code (i.e. not have to routinely perform work outside normal working hours, not to be penalised for refusing to attend to work matters outside normal working hours and the duty to respect another person's right to disconnect).

8.3 Notwithstanding the above, in the absence of a dividing line between the workplace and the home, some employees struggle to find a balance between their work and home life. Employers will not be positioned to monitor and enforce requirements for regular breaks or recommendations to leave the workspace for a period.

9. Data Protection and Data Security

9.1 A key concern for employers is how the business can ensure and monitor compliance with its legal obligations when employees are working remotely. Data protection is of particular concern given the extent of obligations under the GDPR and the Data Protection Act 2018.

9.2 Many employers may already have policies in place to manage remote working which address data protection obligations. For those who do not, the DPC's guidance for data controllers (which include employers as controllers of personal data, including any personal data processed by the employee in the course of their employment when working remotely) may be helpful.

9.2 Any COP guidance around compliance with data protection obligations should address what must be included in employers' data protection policies and privacy notices in order to address issues arising from remote working arrangements.

9.4 ***Relevant DPC Guidance***

1. **Guidance for Controllers on Data Security, February 2020**
   (the "**Data Security Guidance**")

   While the Data Security Guidance provides a helpful overview of relevant measures, more detailed guidance is required to ensure that employers and employees implement and maintain the required data and cyber security standards when engaged in remote working.

2. **Protecting Personal Data When Working Remotely, March 2020** (the "**Remote Working Guidance**")

   The Remote Working Guidance sets out practical tips around how to keep personal data safe when working remotely and addresses device use, sending/receiving emails, cloud and network access and dealing with paper records.

   Updated practical guidance would be helpful now that remote work is a more permanent feature as again, it is vital that both employers and employees comply with all applicable data protection obligations.

3. **Data Protection in the Workplace: Employer Guidance, April 2023** (the "**Workplace DP Guidance"**)

   This recent guidance clarifies the practice of implementing security measures (considered in the Data Security Guidelines) in the workplace, including remote workplace settings.

10. Cost

10.1 A financial burden is connected with the provision of infrastructure and appropriate remote data security to successfully manage remote working arrangements. Smaller employers, in particular, may struggle to fund the cost of setting up an on-site workstation and a remote workstation for employees. Clarification is needed on the apportionment of home utilities for permanent remote working arrangements.

11. Flexible Working Arrangements

11.1 The Committee has noted that the WRC has been directed to prepare a Code of Practice on the Right to Request 'Remote Working' which appears to exclude the right to request 'Flexible Working'.

11.2 The Committee further notes that Part IIA of the 2023 Act, dealing with the Right to Request Flexible Working, also requires employers to consider a Code of Practice, when considering the termination of a flexible working arrangement.

Conclusion

The Committee is available to provide any further information which may be required by the WRC in support of this consultation process and to assist in the development of the COP if that would be helpful.

For further information please contact:

Fiona Cullen
Head of Policy & Government Affairs

f.cullen@lawsociety.ie

Blackhall Place, Dublin 7
t. 01 672 4800
e. general@lawsociety.ie