Public Consultation on Guidance for Remote Working
Submission of Impact Privacy

IMPACT PRIVACY
Bringing privacy to life

IMPACT PRIVACY
Bringing privacy to life

Remote Working Guidance Consultation
Enterprise Strategy, Competitiveness and Evaluations Division
Department of Business, Enterprise and Innovation
23 Kildare Street
Dublin 2

22 July 2020

Dear Sirs

Written Submission by Impact Privacy: Remote Working Guidance

Impact Privacy is an advocate for more flexibility in where, and when, employees undertake their work for employers. We believe the economic, business, social, and environmental benefits of flexible and remote working outweigh any associated disadvantages. Consequently, there is considerable merit in providing comprehensive support and guidance to both employers and employees in the effective move to, and subsequent management of, remote working.

Data protection and privacy should not be a barrier to remote working or used as an excuse to unduly limit its scope. This means providing data protection guidance that is practical, comprehensive, and easy to follow. It also requires avoiding the conflation of general data protection risks (that are not unique to remote working) with risks that arise mainly in connection with remote working.

Our response reflects this and specifically focusses on data protection and the needs of the SME sector in particular. SME's make up 99.8% of the total number of enterprises in Ireland, but in the vast majority of cases they do not have the means or resources to respond to regulatory risks (like data protection) in the same way as large enterprises. This means SMEs have a far greater need for reliable, up-to-date, and comprehensive advice from the Government and its agencies to properly, and positively, respond to social initiatives.

We have attempted to keep our comments concise and insightful, and these can be found on pages 3-5 below.

Yours faithfully

Léon Atkins
Chief Executive

For and on behalf of
The Impact Privacy Team

Who is Impact Privacy?

Impact Privacy delivers privacy and data protection solutions to micro, small and medium-sized businesses globally. Based in Ireland and North America our services include privacy risk management, privacy solutions and the provision of privacy operations through our managed services.

A resource that is comprehensive and focussed

Clarity and certainty cannot be achieved through guidance that simply refers to disparate resources of information.

Instead, we advocate the development of a discrete and specific resource that addresses remote working coherently and comprehensively, in a way that overcomes the potential complexity of a transition to remote working[1].

This means:

- developing a single comprehensive repository (such as a website) as the primary resource for addressing remote working risks, with references to other materials being limited and focussed on exceptions or areas of particular complexity;
- ensuring the resource addresses the issues specifically associated with remote working;
- providing resource materials that practically support a transition to remote working (for example, through template policies); and
- operationalising the resource materials as a set of consolidated key steps, actions, and considerations, culminating in a checklist which facilitates (i) due consideration of remote working initiatives; and (ii) their subsequent effective design and implementation.

The initiative of the Small Firms Association[2] is an example of a similar resource and demonstrates the possibilities for a resource of this nature.

Guidance and resources should give certainty

We believe Government guidance and resources should, if followed and used, provide some certainty the relevant risks are being managed in a way that meets the expectations of applicable regulations and standards. The guidance and resources should not give rise to adverse consequences, be ambiguous, or simply rehearse the regulations and standards that apply.

In respect of data protection, this means advocating an approach consistent with the Data Protection Commission's ("**DPC**") proposed Regulatory Strategy 2020-2025, specifically in respect of Outcome 2:

There is clarity and certainty in how data protection law is applied.

This means:

- engaging the DPC in the Remote Working initiative as a key stakeholder from the outset in a way that recognises the influence its guidance will have on the protection of personal data when remote working; and
- the DPC acknowledging how its guidance can provide assurance in meeting regulatory expectations.

Conflation of issues should be avoided

Our belief is the value of remote working requires employers to give due and objective consideration to any remote working initiatives.

Whilst any guidance or resource should address key concerns that employers may have, it should also avoid conflating general good business practices with those specific to effective, safe, and compliant remote working. This will ensure employers better understand the specific issues associated with remote working, how those can be overcome and the overall impact they may have on the business.

By way of example, we note that the DPC's remote working tips[3], and its accompanying infographic, include measures that represent general good data protection practice. These tips may have been more useful if they highlighted and addressed the very particular data protection risks associated with remote working.

[1] Remote Work in Ireland, Future Jobs 2019 (page 52): "multiple stakeholder groups identified the absence of official guidelines...on the topic of remote work. [Many employers] are unclear how to manage the various aspects of what this entails.

[2] See page 31 of Remote Work in Ireland, Future Jobs 2019

[3] "Protecting Personal Data When Working Remotely" 12 March 2020

Give guidance on simple measures that can be taken to manage data protection risks

Many data protection risks can be effectively managed through simple measures which, if positively addressed in the guidance, can help overcome myths and other perceived issues associated with personal data and remote working.

For example:

- key steps to maintain confidentiality of data in the home or other working space; or
- the safe use of employer provided IT in remote working environments;

Provide more detailed and practical guidance on specific remote working risks

The DPC's remote working tips do not comprehensively deal with the practical issues specifically associated with remote working. Any future guidance or resource should address at least the risk areas described below.

Use of video conferencing

The DPC's Data Protection Tips for Video-conferencing are not referred to in either the DPC's remote working tips or the Guidance for working remotely during COVID-19.

Any guidance should include clear advice on the risks associated with video conferencing and the key steps an organisation should take in:

- selecting a provider;
- setting up the video-conferencing facility;
- deploying the facility;
- using the facility; and
- using specific features, such as recording.

Use of employee devices

Employees using their own devices may be considered by some employers as an inherent part of facilitating remote working. The risks associated with this strategy and how they should be overcome (or avoided) should form part of the key considerations included in any guidance.

Special categories of personal data

Any guidance should address the issues associated with the use of special categories of personal data (like health data) or sensitive data (like bank account details) in the remote working environment.

Information security risks

Whilst the DPC's remote working tips provided some useful guidance on the security measures to be adopted for remote working, that guidance was not comprehensive and referred to the DPC's full guidance note on data security[4].

Whilst the data security guidance note referred to remote access, it was not specifically developed to address remote working risks.

We believe it would be helpful to describe the principal information security risks associated with remote working and provide specific guidance on how to respond to those risks.

Guidance must be easy to find, accessible and updated regularly

We have noted that in many cases existing guidance is not easy to find or is inaccessible.

For example, the DPC published its guidance and tips for remote working and video-conferencing as blogs. These blogs are not linked to the DPC's "For Organisations" pages and are not referred to in the "Guidance" pages[5].

For any guidance to be of value it must be easy to find and accessible. This means publicising the guidance and ensuring it is intuitively located on relevant websites, preferably in a single websource (see "A resource that is comprehensive and focussed" above). This is particularly important when those seeking to use the guidance may not be familiar with the sites where the guidance is to be found, or the issues on which they are seeking support.

[4] "Guidance for Controllers on Data Security" February 2020

[5] There is a link to the blog page in the Guidance page for DPOs

Develop guidance for employees seeking to switch to remote working

Employee's need to be comfortable that remote working will not adversely affect their ability to do their job, and that they understand the impact of remote working on how they do they job. We also believe that employees will want to actively support their employers effect the successful transition to remote working.

To do this we believe separate guidance and resources for employees is required to be made available. This should:

- provide employees with access to the information and resources necessary to promote the positive consideration of a transition to remote working ("why remote working and how to do it"); and
- give comprehensive guidance on the do's and don'ts of remote working, including on issues that may commonly be perceived as barriers by employers.

Impact Privacy, 22 July 2020


info@impactprivacy.com


Europe: +353 (0)1 554 1189
Americas: +1 800-909-1189


www.impactprivacy.com