Risks and opportunities of the GDPR

Microsoft | oakton

IS YOUR BUSINESS READY FOR THE GDPR AND ITS TOUGH NEW DATA PROTECTION LAWS?

There is a lot of noise in market about the General Data Protection Regulation (GDPR). And rightly so. The GDPR represents a new global high-water mark for data protection and privacy regulation, imposing new and complex privacy and cybersecurity rules on thousands of organisations around the world.

The new laws, in place from 25 May 2018, expose organisations to significant risk and heavy fines – if found to be non-compliant.

Given the risks, we propose some questions that every organisation should be asking:

- Is your organisation affected by GDPR?
- How do you know if your existing systems comply?
- What is the cost of non-compliance versus compliance?
- Who can you trust to partner with you on GDPR compliance?

This eBook provides an overview of the GDPR and its effects; as well as providing some insights and recommendations around what needs to be done if your organisation is affected.

THE STORY BEHIND THE GDPR

The European Union – the driving force behind the GDPR – has always been regarded as a leader in data protection. Back in 1995, it adopted the Data Protection Directive to protect citizens' data in the early years of the Internet. More recently, to address the rapid growth in use of digital information, the EU proposed a comprehensive reform of its Data Protection Directive.

Following extensive review, the GDPR was introduced in 2016 to reinforce existing rules and bring in new ones to protect people's rights when it comes to their personal data.

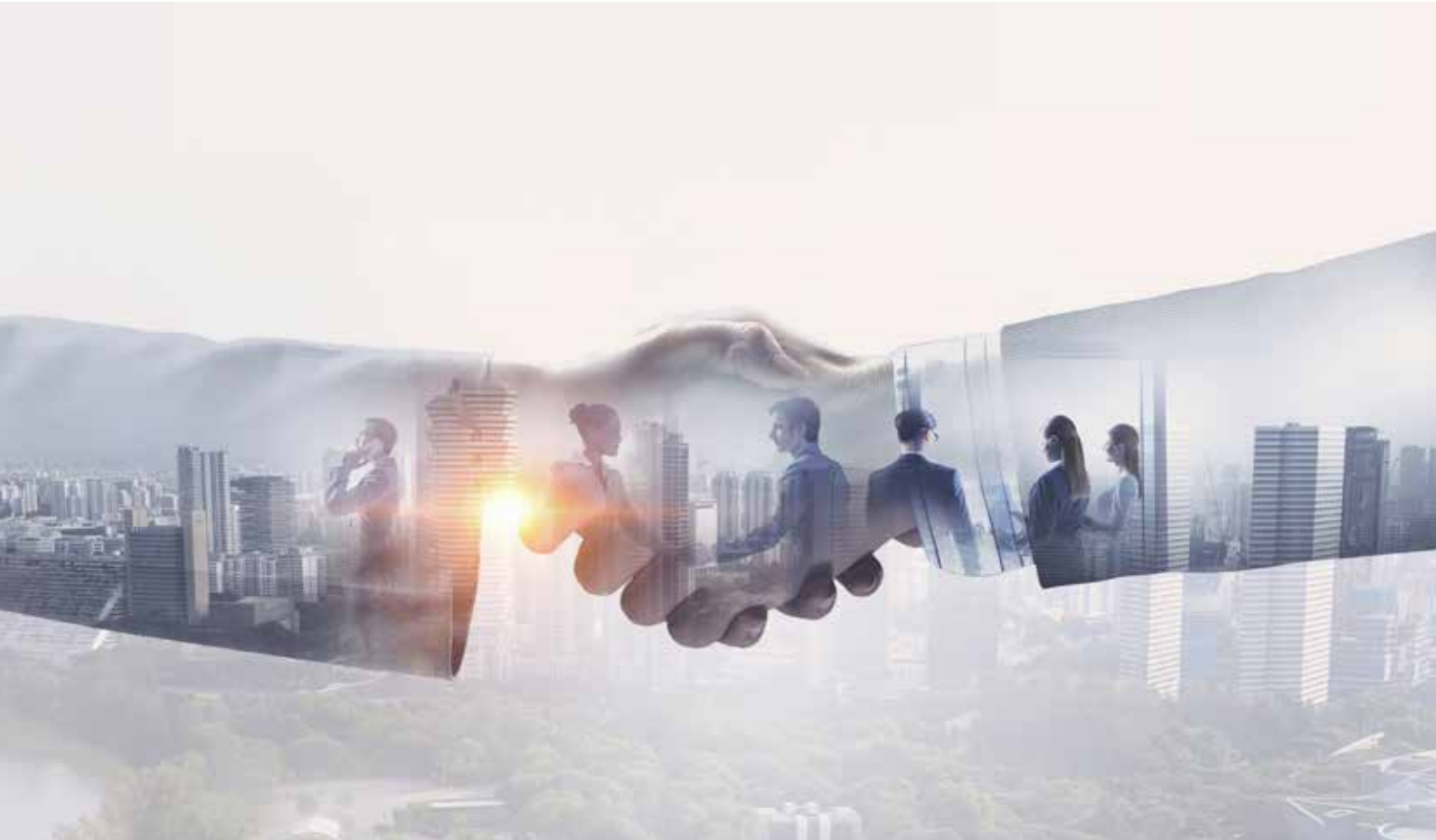
UNDER THE GDPR THERE ARE SOME KEY REGULATIONS AROUND PRIVACY AND SECURITY DATA HANDLING

These include:

- **Specific consent for each purpose of personal information usage** – organisations must request consent for each additional purpose for which existing data collections are used
- **Extended data rights (in addition to those already in the Australian Privacy Act 1988 (Cth) for individuals** – including rights to access all information stored about themselves, to data portability, to alter stored data and to cease processing altogether
- **Rights around automated profiling** – individuals may request information on how profiling decisions are made (potentially including details of the computer rules involved) and which data was used to arrive at the profiling decision
- **Data security protective controls** – including secure configuration and user access management
- **Incident response** – including a continuous monitoring ability to detect potential or actual breaches of personal information and to notify authorities within 72 hours of an incident

These new rights significantly raise the bar for data protection. Recognising that it would take some time and effort to realign organisation-wide systems to meet the new rules, the EU voted to give organisations two years (until 25 May 2018) to modify existing data systems. Beyond that date, any eligible organisations face fines of up to €20 million or up to 4% of total worldwide annual turnover (whichever is higher) if they fail to comply with the GDPR.

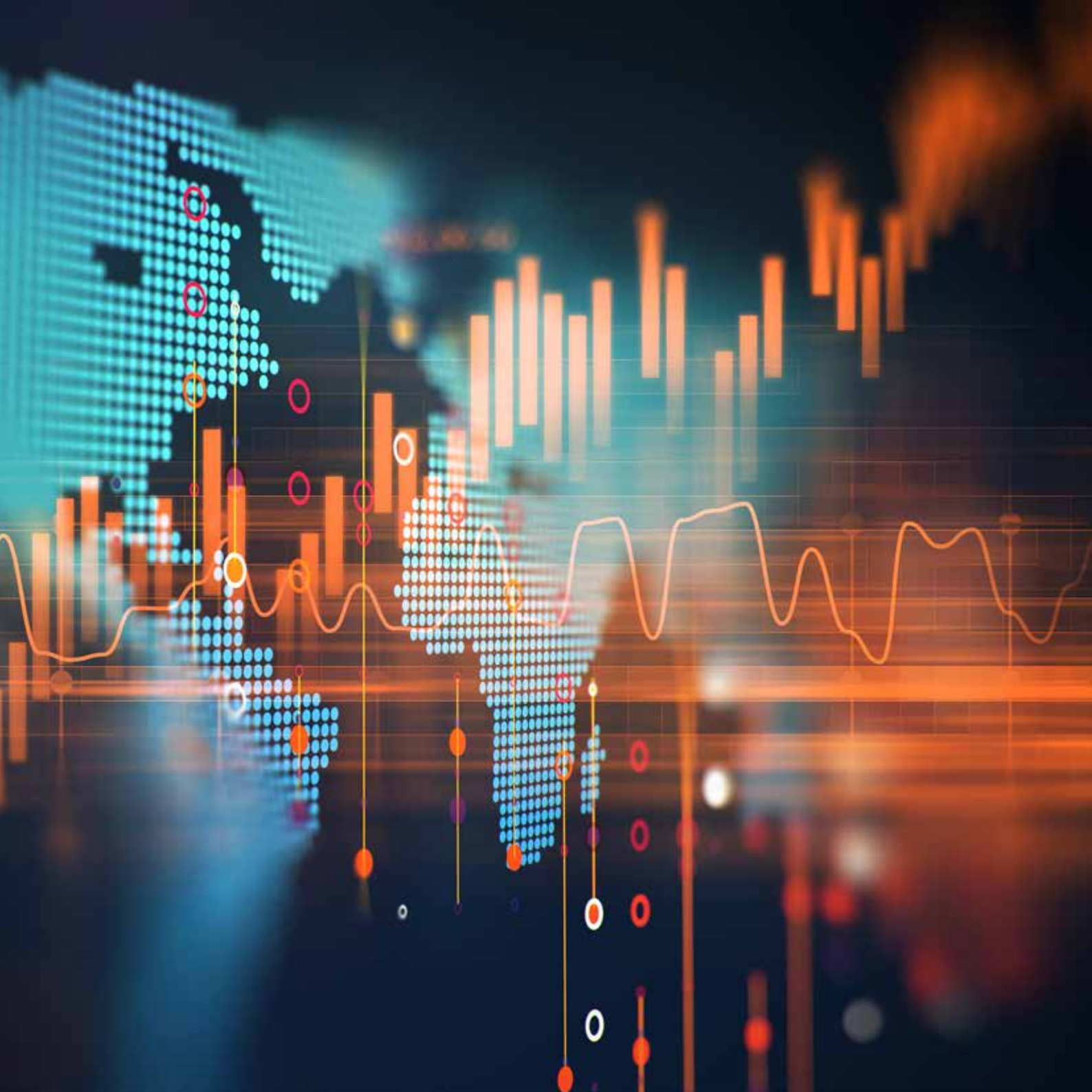
With the GDPR, the EU has set a new, higher benchmark for data protection. It is quite likely that other jurisdictions around the world will use it as a framework to re-align their existing data protection and privacy legislation. This could ultimately mean that even more organisations, not just those directly affected by GDRP now, will need to uplift their privacy governance and supporting cybersecurity controls to bring them in line with possible future regulations.



WHO IS AFFECTED BY THE GDPR?[1]

- Any local firm with digital operations selling goods and services which are offered (actual sales, payment and delivery are not required) to EU residents is affected by the GDPR. It relates to the GDPR's concerns over 'monitoring' – the retention of simple cookies or other web tracking methods, the creation of customer and marketing profiles, and the use of these profiles and tracking data to make decisions concerning the individual or for analysing or predicting their personal preferences, behaviour and attitudes.
- Any firm that is the local arm of a multinational enterprise, which may store or process data relating to EU citizens ('data subjects') widely within the organisation, including in Australia, is affected by GDPR.
- Finally, any firm that is a service provider to a global organisation, and is a 'data processor' to its customer, the 'data controller' (to use GDPR terminology), is affected by the GDPR. For example, if a global finance company sub-contracts local email marketing to an Australian agency, and this agency deals with data subjects from the EU, then it is a data processor and must be GDPR compliant.

1 Microsoft and Oakton provide consulting advice and recommendations regarding your compliance status and overall readiness but it is not actual certification of GDPR compliance. Neither this document nor the assessment service are legal advice nor are they intended to be comprehensive. You should seek such legal and other professional advice as may be required for your individual circumstances. It might not be sufficient for you to rely on this document or the assessment service alone.



GDPR COMPLIANCE = COMPETITIVE ADVANTAGE

Trustworthiness is intrinsic to building business value in a digital world. And privacy and security are increasingly important determinants of trustworthiness – when you get them right, you maintain a solid reputation in the marketplace. While the new rules of the GDPR may seem tough, they represent the pinnacle of trust between an individual and an organisation. These rules require a level of data protection and security that every organisation should aspire to, whether in-scope for GDPR compliance or not.

The ability to demonstrate compliance with GDPR offers organisations a distinct advantage. Thus, it may pay to re-evaluate your data protection and security systems in line with the new standards regardless of whether you deal with any EU residents' data. The GDPR is globally recognised as the gold standard for data protection and the ability to demonstrate compliance will instil trust in your employees, suppliers, business partners and customers.

ORGANISATION ASSESSMENTS ARE KEY

It is critical that organisations are performing the 'privacy by design' assessments required by GDPR. These rigorous assessments – which involve mapping exercises to document where and what kind of data they store and process, the business purposes of that data and the cost/benefit analysis of why such data is held – take time, yet are a critical first step in GDPR compliance.

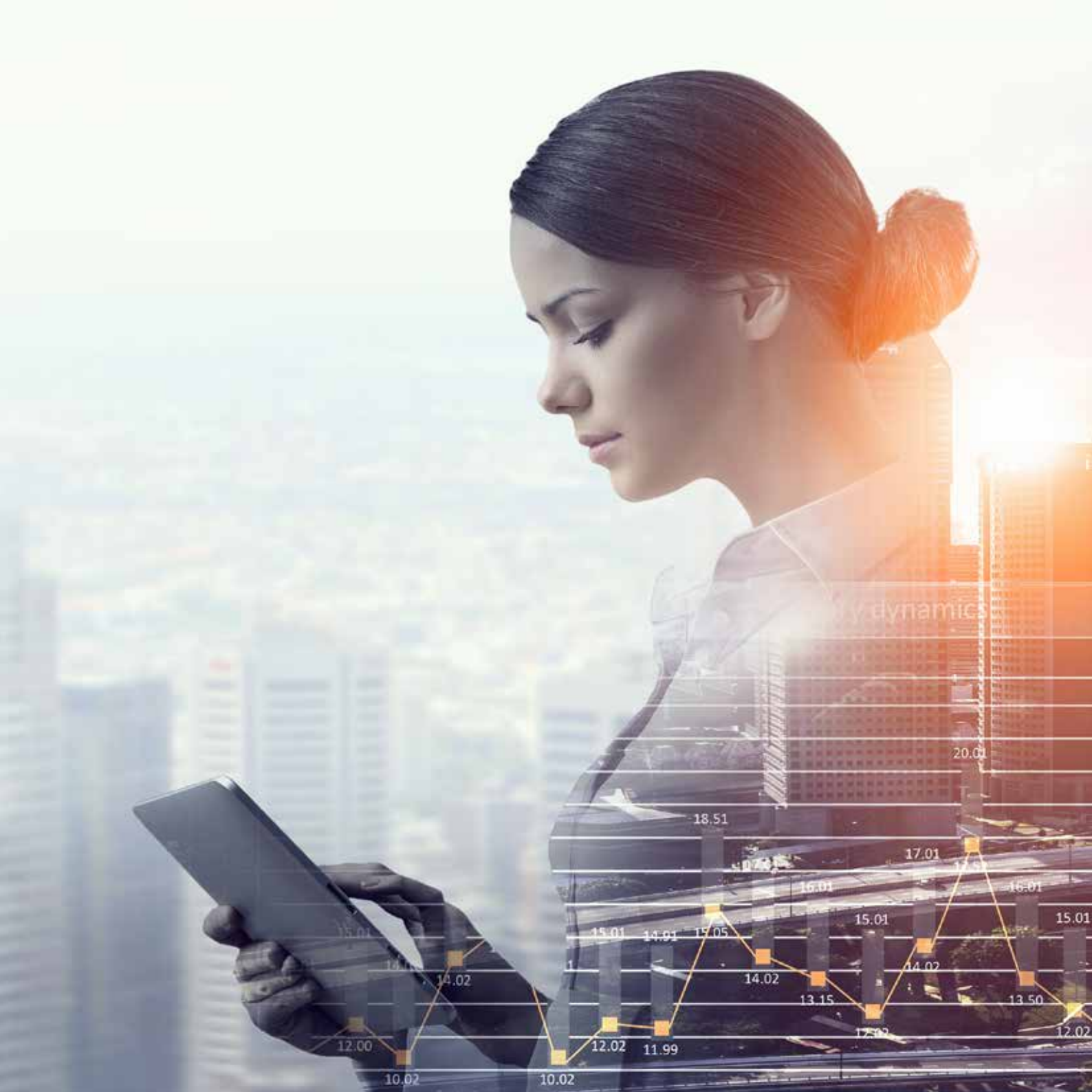
With the spotlight on data security – and the accompanying empowerment of individuals when it comes to their personal data – the business case for GDPR compliance is imperative. Regardless of whether you fall into the scope of GDPR eligibility or not, Microsoft and Oakton recommend that you should:

1. **Perform an assessment to determine your role in GDPR** – are you a data processor? A data controller? Do you need to appoint a Data Protection Officer? It is important to understand your organisational role in relation to the GDPR before you start evaluating your systems and processes. It is recommended that you look at the way you share data with suppliers, too.

2. **Audit your data processing activities** – do you have control over the personal data you collect, the way you capture individuals' consent around the handling of that data, and how that data is shared? Are your data protection policies compliant?

3. **Define a roadmap for GDPR compliance** – if any gaps are identified between your current state and where you need to get to, how will you get there? What new systems, procedures and controls need to be put into place? What is the cost? How will you be able to provide evidence of your GDPR compliance?

These steps can be complex and we are here to help navigate this with you.


18.51
17.01
16.01
15.01
15.01
14.02
13.15
13.50
12.02
12.00
10.02
10.02
12.02
11.99
20.01

OAKTON GDPR READINESS REVIEW

Oakton, in partnership with Microsoft, provides an end-to-end assessment of your organisation's readiness to meet GDPR requirements.[2] We will look at your overall privacy and security governance controls, and provide reputable recommendations on not just how to uplift any weak areas in terms of GDPR readiness but also the broader data management and application support capabilities around your organisation's privacy and regulatory needs. We also conduct a detailed, script-driven, technical review of your database environment to check its current overall health and identify any issues that constrain adoption of the measures as a recommendation of what might be required to become GDPR compliance ready.

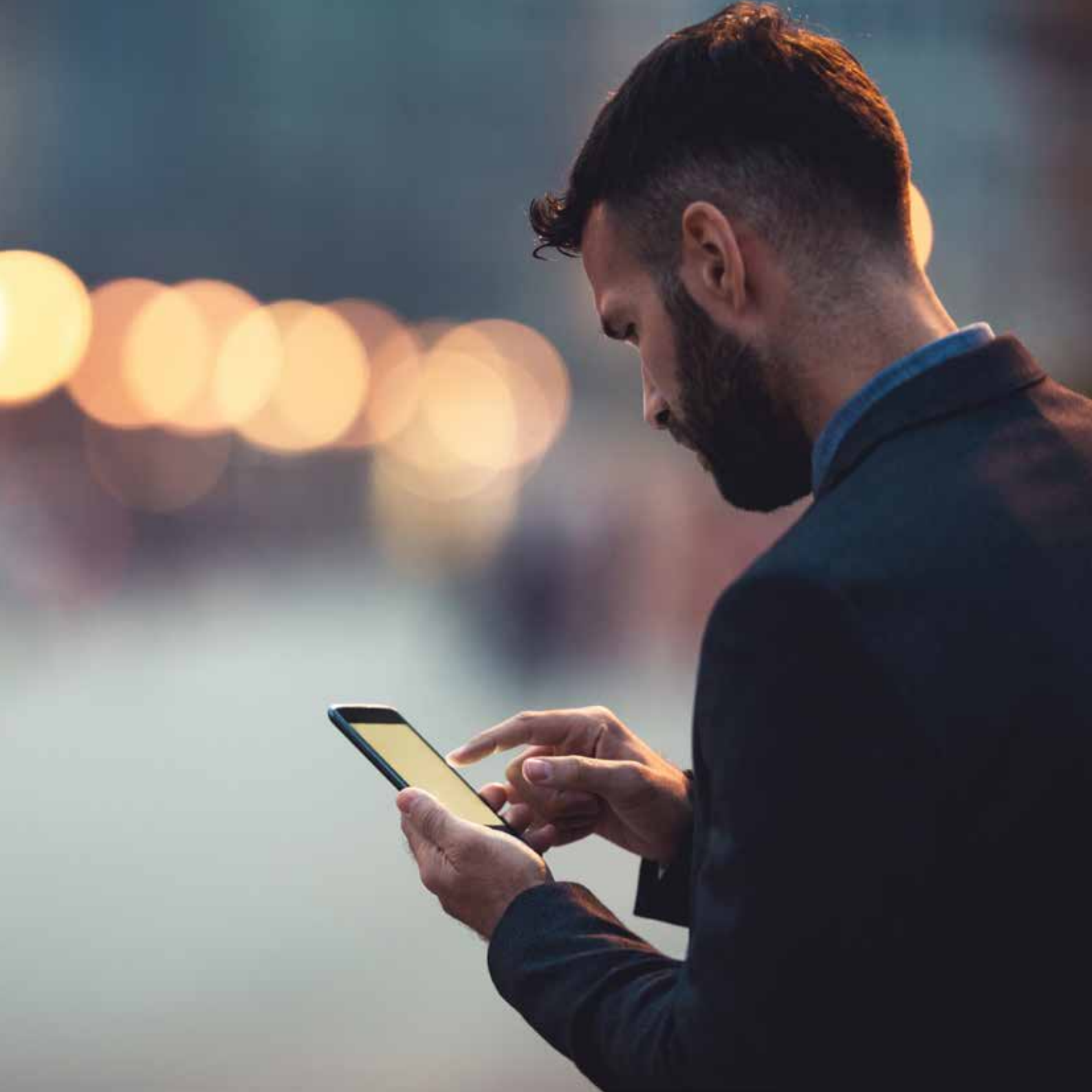
Oakton will assess your GDPR readiness in eight domains of data privacy and security governance:

1 Governance & Awareness
2 Policies & Procedures
3 Third Party Controls
4 Data Subject Management
5 Risk Management
6 Security Access & Event Management Controls
7 Incident Management
8 Compliance

These 8 domains are broken down into 80 controls, which are explicitly cross-referenced to specific GDPR Articles and recitals. Where the control includes significant technical dimensions (database configuration, system logging or encryption, for example), we assess these as well. For all controls, Oakton will provide a description of the current status of compliance as well as a recommendation for any improvement considered necessary.

You will receive a written report with a prioritised roadmap of recommended actions for all controls – both business and technical. This will provide you with a recommendation on how to become more GDPR ready.

2 Microsoft and Oakton provide consulting advice and recommendations regarding your compliance status and overall readiness but it is not actual certification of GDPR compliance. Neither this document nor the assessment service are legal advice nor are they intended to be comprehensive. You should seek such legal and other professional advice as may be required for your individual circumstances. It might not be sufficient for you to rely on this document or the assessment service alone.



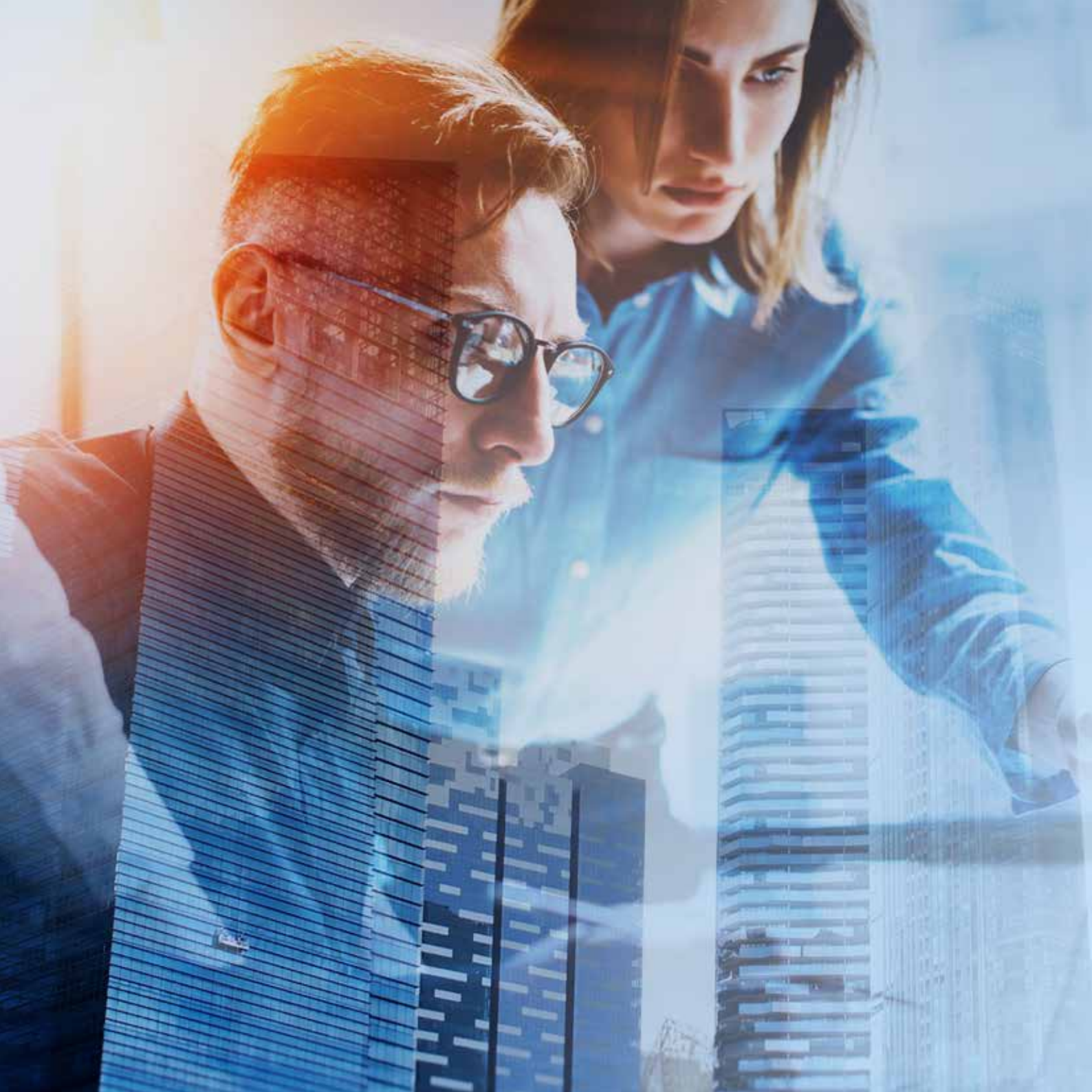
WHY OAKTON AND MICROSOFT?

Through our partnership with Microsoft, Oakton gains access to Microsoft's exclusive IP and emergent technologies that focus on GDPR. You gain the advantage of our expert local knowledge backed by a global partner at the forefront of GDPR compliance assessment.

TIME TO ACT NOW?

Call us today and we will show you how to set your organisation on the path towards GDPR compliance. Our assessment will help you to have the most up-to-date data privacy protection and security processes and systems that will provide you with a comprehensive way forward on the GDPR.[3]

3 Microsoft and Oakton provide consulting advice and recommendations regarding your compliance status and overall readiness but it is not actual certification of GDPR compliance. Neither this document nor the assessment service are legal advice nor are they intended to be comprehensive. You should seek such legal and other professional advice as may be required for your individual circumstances. It might not be sufficient for you to rely on this document or the assessment service alone.



Adelaide

+61 4 3304 5022
Level 3, 190 Flinders Street
Adelaide SA 5000

Brisbane

+61 7 3136 2900
Level 22, 141 Queen Street
Brisbane QLD 4000

Canberra

+61 2 6230 1997
2/45 Wentworth Avenue
Kingston
Canberra ACT 2604

Melbourne

+61 3 9617 0200
Level 8, 271 Collins Street
Melbourne VIC 3000

Perth

+61 8 9222 8300
Level 10, 66 Street
Georges Terrace
Perth WA 6000

Sydney

+61 2 9923 9800
Tower 3, Darling Park,
201 Sussex Street,
Sydney NSW 2000