NEWS

FIXED PRICE SEAMLESS BOOKKEEPING HAS ARRIVED

#seamlessbookkeeping

Zip through your work with #seamlessbookkeeping with the new AdvanceTrack® Cloud Platform. Fully Managed Seamless Bookkeeping in the Cloud run by Professionals.

Call +44 (0) 24 7601 6308

advancetrack® outsourcing

T: advancetrack® on +44 (0) 24 7601 6308
E: advice@advancetrack.com
W: www.advancetrack.com
@AdvanceTrack

University of Warwick Science Park, Sir Williams Lyons Road, CV4 7EZ, UK

NEVER KNOWINGLY BETTERED
For Quality | For Security | For Service & Reliability

THINK OUTSOURCING. THINK ADVANCETRACK®

ISO/IEC 27001 Information Security Management
ISO 9001:2015 Quality Management
Xero Certified Advisor
Intuit Certified ProAdvisor QuickBooks Online
ICAEW Chartered Accountants

InsideOUTSOURCING®

The Newsletter for Forward Thinking Professionals • 2017 // Issue 4 • www.advancetrack.com

Fully managed outsourcing. Not an App in sight!

☑ UK Headquartered ☑ ICAEW Member Firm ☑ Run by UK Qualified Chartered Accountants
☑ ISO9001:2015 Certified for Quality Management ☑ ISO27001:2013 Certified for Information Security
☑ Secure platform with full job management ☑ Job tracking as standard since 2006
☑ Process Driven Mass Customisation

NEWS

Practice Compliance Outsourcing

Final accounts production • Personal tax returns • Corporation tax returns
HMRC-recognised iXBRL tagging services • Payroll • Cloud Bookkeeping

Call +44 (0) 24 7601 6308 | www.advancetrack.com

advancetrack® outsourcing

The EU General DATA PROTECTION REGULATION

This will become law regardless of the UK's continuing membership of the EU. It is also likely that to trade with individuals and organisations within the EU, post Brexit, UK businesses will need to be compliant with these regulations. The GDPR will apply in the UK from 25 May 2018.

Should we be scared by the new regulations?

With a potential fine of 4% of global turnover or €20m we need to ensure that we understand how it impacts on us as professional firms. If you outsource, you need to consider carefully if your outsourcing supplier is able to allow you to remain compliant. Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Do we know what actions to take? Let's see what you need to know.

Data Protection Officer

Accountability is a key component of the new regulation. In certain circumstances, data controllers and processors must appoint a Data Protection Officer ("DPO") as part of the organisation's accountability.
The following are circumstances where an organisation needs to have a designated DPO:

a. Processing carried out by a public authority;
b. The core activities of the controller or processor consist of processing requires regular and systematic monitoring of data subjects on a large scale; or
c. The core activities consist of large scale processing of special categories of data.

The DPO may be employed or on a service contract, but is required to have enough expert knowledge, dependent on the activities for which they are responsible. This DPO may act for a number of undertakings.

Territorial Reach

The GDPR also impacts on processors of data outside the EU, so this will impact on all outsourcers in popular locations outside the EU such as India. Processing activities relating to the offering of goods and services (even if free) or monitoring the behaviour of EU data subjects (within the EU). Many will need to appoint a representative in the EU. Most outsourcers will for example, have no presence in the EU. In such circumstances, firms using a provider that is not compliant could be breaching the regulations. Companies outside the EU targeting customers within the EU will be subject to the GDPR, which is not the case currently.

The Role of the Data Processor

The GDPR requires data processors to have direct obligations for the first time. This includes an obligation to maintain a written record of processing activities carried out on behalf of the data controller, appoint a DPO where required and notify the Data Controller of a personal data breach without an undue delay. Provisions related to cross border transfers will also apply to processors.

Supply and commercial agreements will need to be reviewed to accommodate the new regulations.

Accountability

The Data Controller has onerous obligations to demonstrate compliance. This can include:

a. Maintain documentation.
b. Carry out a data protection impact assessment for more risky processing.
c. Put in place data protection by design and default.

Fair Processing Notices

When personal data is obtained, the Data Controllers must provide transparent information to data subjects. Existing forms of fair processing notice will need to be reviewed as the GDPR is more detailed than currently in place. Information to be given to the data subject is more comprehensive than is currently the case (including for example, the ability to withdraw consent) and the period for which data is stored.

Data Controllers will need to provide information in a clearly accessible format in a clear way with the new GDPR obligations in mind.

Consent

It needs to be as easy for a data subject's consent for processing to be withdrawn as it is to obtain consent. The data controller will be mandated to demonstrate that consent was given and whilst existing consents may work, they need to meet the new conditions. There are areas concerning personal data used for direct marketing and also the age of parental consent where there is no clarity on whether the age is 16. Some member states can lower this to 13. We will look at this further in a future newsletter or on our website in the coming months.

Fines

There will be a tiered approach to the way penalties for breaches are imposed. This will enable DPAs to impose fines of up to the higher of 4% of global revenue and €20m (for example, breaching the requirements relating to international transfers or basic principles for processing, such as conditions for consent).

There are other specified infringements which attract fines up to the higher of 2% of global revenue and €10m. These fines apply to an "undertaking" and this was clarified in Articles 101 and 102 of the TFEU.

"The One-Stop Shop"

A company operating in many EU countries would generally only deal with one lead DPA. There has been a degree of criticism. In order to address some of this criticism, the GDPR allows individuals to have their cases dealt with locally, with the Lead Authority and Concerned Authorities working together. It is to be hoped that when in place, that it does not lead to forum shopping.

Removing a Notification Requirement

There will no longer be a requirement for a data controller to notify or seek approval from the DPA in some circumstances. Whilst this may reduce a financial and administrative burden, this may lead to some DPAs seeking alternative funding. The policy now is for Data Controllers to put in place effective procedures and mechanisms to focus on higher risk operations and undertake a data protection impact assessment. This should consider severity and likelihood of risk, especially with large scale processing. A lot of effort is required and the potential fines are such, that they may outweigh the benefits. Also, a new requirement to consult the DPA in advance where the data impact assessment may indicate high risk if measures are not taken. If the DPA considered the processing may breach the GDPR, they could give written advice or use their enforcement powers may have multiple impacts, either nothing is high impact(!) If your outsourcer, for example uses e-mail and tools such as DropBox to exchange confidential data, you may need to consider if that places your firm at risk of fines were there to then be a data breach.

European Data Protection Board ("EDPB")

The independent EDPB will comprise of the EDP supervisor and senior representatives of the national DPAs. Its role will be to issue guidance and opinions, reporting the EU Commission and applying the GDPR consistently across the EU.

International Transfers

The way that consent is dealt with for data exporters has changed. Moving data outside the EU now requires subjects to have sufficient information on the risks of data transfer outside the EU. This, in the context of outsourcing will require you to ensure that any outsourcer has strong protocols to be able to satisfy yourself of the risks. Consider, for example if an outsourcer using e-mail or DropBox to transfer confidential information is able to satisfy the new requirements.

Data Subjects' Rights

The rights of individuals being strengthened was one of the main aims of this new regulation. This includes, for example, a right to require information about data being processed about then, being able to access such data in some circumstances and correction of data where incorrect. There will also be rights relating to data used for direct marketing purposes. The concept of data portability has also been created allowing individuals to receive back their personal data in a structured and commonly used format to allow it to be more easily transferred to another data controller. The CJEU decision on the Google v Spain case and the "right to be forgotten" or "right of erasure" received the most attention. This allows individuals to require the data controller to eras such personal data without undue delay in certain situations, such as withdrawing consent. Following this, there is an obligation to advise 3rd parties that the data subject has requested erasure of any links to, or copies of that data. This may in practice be difficult to manage. There is a requirement for the data controller to respond within one month, with more complex requests allowing this to be extended. Clear processes will need to be in place to meet such obligations and provided free of charge unless the request is "manifestly unfounded or excessive".

Six Things you should do now to be ready for GDPR

1. Embrace Privacy by design • When a new process or product is deployed, ensure that privacy is embedded into the process. Considering the process early on will enable this to be both structured and validation checks to be put in place.
2. Understand the legal basis on which you use personal data • Consider engagement letters and contracts as this may often be your form of consent for processing if withdrawn. The documents should demonstrate that the consent is given freely, is specific and informed and the burden of proof will be on the data controller, for example, the accounting firm. Obtain legal advice on how you would deal with any withdrawal of consent.
3. Review your privacy notices and policies • Policies need to be transparent and easily accessible. Information provided need to be in clear and plain language.
4. Accountability framework • Clear policies need to be in place to meet the standards.
5. Review the data subjects' rights • Data subjects may exercise their rights such as data portability or the right to erasure. If personal data is retained, consider what legitimate grounds there are to retain this. The burden of proof to demonstrate your legitimate grounds for retention override the interests of data subjects.
6. Prepare for data security breaches • Clear policies and practised processes need to be in place in order to react quickly to any data breach to ensure that timely notification is made where required.