Insight Guide

Is your institution achieving compliance when recycling ICT assets?

Will Brexit have an impact on data protection legislation

Supported by

LiFE Framework:

Sustainable ICT

Times are changing

The world of technology has advanced beyond measure since the original EU Data Protection 95/46/EC came into force way back in 1995. Back then in the land before smartphones, the 'cloud' was just something that blocked out the sun.

So with mind-sets to privacy evolving rapidly since those days, the law was updated in 2016 law with the intent to reflect these vast changes in technology and our use of it. This in turn means that your business or organisation's ability to demonstrate compliance with the new data protection legislation is paramount in order to maintain a healthy reputation and not succumb to a possibly crippling financial punishment because of a data breach. While Brexit has cast uncertainty over what legislation will apply in future, there will continue to be regulations in this area that are likely to closely mirror those adopted in the EU to facilitate cross-border trade. While the regulatory future is uncertain, the continued need for effective data protection is as essential as ever.

How this applies to you

As individuals we have a nature to consume resources at an alarming rate. For ICT equipment, not only has there been a predisposition to demand the latest and greatest technology, but there has also been refresh catalysts driven by the manufacturers, resellers and software developers. This has created a "use and lose" approach to hardware. Within the wider world of ICT, the perception is that once infrastructure has finished its life, then it is simply waste and those who remove it are the "ICT Dustmen". However, a failure to understand that disposal includes three assets – data, software as well as hardware – leads to poor policy, poor operational process and most of all, to uncontrolled risk taking.

This often-maligned process continues to allow data to leak from business unabated. Within the last few years the UK Information Commissioner has levied fines of over £500,000 for data breached as a result of this process. In the US, a leading drinks manufacturer suffered a significant breach when a staff member stole redundant equipment rather than place it into the disposal route. So how can such a seemingly innocent process go so badly wrong?

Registered Office : EAUC UK Office, University of Gloucestershire, The Park, Cheltenham, GL50 2RH
Tel : 01242 714321, info@eauc.org.uk, www.eauc.org.uk

Company Limited by Guarantee in England & Wales No : 5183502 Charity No : 1106172
Printed on 100% recycled paper

Insight Guide

To understand this let us first define asset disposal. The Asset Disposal & Information Security Alliance (ADISA)'s definition is as follows:

"Any situation where the data controller transfers custody of an ICT asset to a third party for management or processing, whether on a temporary or permanent basis."

Therefore, your institution would be considered the "data controller" and your IT/WEEE recycling partner would act as the "data processor"

Whilst technology has changed dramatically in the last decade, the business process of disposal has not. Not only does this process now include different product types, but also different media. Magnetic hard drives are the default media, but with increased usage of smart phones and tablets, solid-state media is becoming more prevalent. We mustn't forget tape either!!!

Companies historically may say "our policy is to destroy all hard drives", this will no longer cover all potential outputs from business or all data carrying media. The recent fine on a UK central government department for the loss of an unencrypted back up hard drive shows that data protection efforts must focus on all areas where data carrying assets are managed, not just whilst on the network. A failure to see the hardware they are disposing of as anything other than "old tin", to view it as waste management, or simply as an asset for resale isn't enough. Higher education institutions must understand that when they release their IT and telecommunication assets they need to apply the same attention to asset management and security as they do to the assets when in life. Asset disposal is an evolving and important business process, which when controlled through an intelligent asset disposal policy can manage risk and promote re-use and therefore create both financial and social benefits.

These significant changes to the law were brought into effect from April 2016 and as an institution within the HE sector you have 2 years to introduce new procedures to meet the new directive. Due to the potential cost implications of these points above it's worth checking that you and your supply chain are conforming to current legislation.

Next steps

ADISA research can evidence that over 66% of UK public sector (on a sample size of over 400 respondents) currently break UK Data Protection law when disposing of ICT assets. As such, despite the EU Data Protection Regulation 2016 being very clear, data controllers have much to do in order to comply with this legislation when disposing of assets, there will be some who will say "so what, we have another law for organisations to ignore".

Not only have the maximum fines (Article 83) increased to €20,000,000 or up to 4% of global turnover but there is also a requirement for mandatory breach notification (Article 33) within 72 hours. Mandatory notification is something already in place in many US states so let us view the EU GDPR definition of data breach:

"'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

ADISA's position is that unless a data controller is able to evidence that they have engaged with data processing in such a way as to be viewed as complying with the EU GDPR then the transaction would be viewed as unlawful, and therefore should be classed as breach. At ADISA we estimate that about 85% of all collections made would currently fall into this category due to the lack of a contract, lack of code of

conduct and certification and lack of formal risk assessments being made. So does the future of asset disposal contain the majority of collections to be classed as data breach and requiring either party to disclose to the relevant data regulator?? It certainly looks that way.

The good news for organisations is that our industry, operating as the final part of the data protection process, has been slowly getting our act together. ADISA Certified companies operate to a rigorous published Standard and more to the point undergo continuous auditing to ensure compliance. The Standard was revised in December 2015 in preparation for the new EU GDPR and throughout the implementation of this law across Europe, ADISA and our members will be working hard to ensure that this is one group which operates to the law and helps their customers comply with law. Since January 2016 ADISA has suspended four companies and permanently excluded one. It makes sense for data controllers that when looking to dispose of ICT assets they should seek to engage with one of the ADISA Certified organisations. Not only will they be able to evidence compliance to the relevant parts of the new EU Data Protection Regulation 2016, but they will also know they are dealing with the industry leading companies to whom they can entrust their brand, reputation and liability without undue concern.

CDL have been ADISA certified members since 2012 and are University purchasing consortium approved to provide this service to your institution.

Further Information

Computer Disposals Ltd (CDL)

www.computerdisposals.com

Email – malcolm@computerdisposals.com

Telephone - 01925 730033

View CDL's corporate video here (under 2 mins) - http://bit.ly/2eK89cl

ADISA

http://adisa.global/company/computer-disposals-limited-cdl/