Centrify
ZERO TRUST SECURITY

Cordery
Legal.Compliance

GDPR Headlines

WWW.CENTRIFY.COM

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation.

Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

From 25 May 2018, new data protection rules called the General Data Protection Regulation (GDPR) will apply across Europe to protect individuals' personal data.

Centrify has worked with the specialist law firm, Cordery, to develop this headline summary of when the GDPR applies, the key impacts and what you need to do to comply with the GDPR. In this note we'll use a few GDPR related technical terms – you can find out more about them here: www.bit.ly/gdprglossary.

The GDPR Will Apply to More Organisations and More Data

The GDPR will apply to:

- not only European organisations, but also to foreign businesses that offer goods or services in the European Union (EU) or monitor the behaviour of individuals in the EU
- organisations of all sizes and types, from public authorities to small and medium-sized businesses to multinationals
- personal data relating to individuals in the EU (even if they are not an EU citizen or resident)
- a wide range of information relating to identified persons or from which a person can be identified, directly or indirectly (which may include IP addresses, and manual records in an organised filing system), and
- a more detailed range of sensitive personal data – including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data or information about a person's sex life or sexual orientation – for which additional protections must be put in place.

There Will Be More Risks but also More Opportunities

The GDPR will also bring with it increased:

- compliance obligations on those businesses that come within its scope
- rights for individuals whose personal data you use
- fines, of up to the higher of €20 million or 4% of global annual turnover for the most serious infringements – not to mention the reputational damage and impact on customer trust, and
- other regulatory activity, including audits and inspections.

But it's not all doom and gloom. There are a wealth of opportunities for forward-thinking companies offering GDPR-compliant solutions.

©2018 Centrify Corporation All Rights Reserved.

What You Need To Do

The GDPR is lengthy and complex but the table following details some key things you'll need to do.

GDPR requirement	GDPR requirement	Why this is important?
Process personal data fairly, lawfully and transparently *(Articles 5(1)(a) and (b), 6-10 and 12-14))*	• Tell people clearly when you collect their personal data how you are going to use this — and don't use it for anything different that the person wouldn't reasonably expect • Get people's consent or ideally ensure you can lawfully process their information on an alternative legal basis	• The more informed and in control of their information people feel, the less likely they are to complain • Each use of personal information / sensitive personal data needs a lawful basis — consent is only one basis and not always the best (because it's difficult to get validly and can be withdrawn)
Only collect and hold personal data which you genuinely need — and destroy data when you don't need it any more *(Articles 5(c) and (e))*	• Build online and manual forms and processes that only collect the minimum personal data you need to collect for the purpose for which you need to use the information • As soon as you don't need personal data any more, destroy it securely • Use anonymised or pseudonymised data wherever possible	• If minimal personal data is retained: - this is less data you have to ensure compliance with the GDPR for (including individuals' rights of access — see below), and - the impact if there is a data breach is reduced • Properly anonymised data is not "personal data" (and the GDPR doesn't apply); pseudonymisation (keycoding) of data is encouraged as a security measure
Keep the data you hold accurate and up to date *(Article 5(1)(d)*	• Build regular reviews, quality checks and data cleansing protocols into database management processes • Prompt individuals to regularly update their information • If someone asks for their information to be corrected / updated, do it quickly (and have a process to support this)	• Incorrect / inaccurate information can have an impact on the individual if this is then used for important decisions that affect them • Inaccurate contact information may mean that important communications or marketing won't reach people

©2018 Centrify Corporation All Rights Reserved.

GDPR requirement	GDPR requirement	Why this is important?
Keep data secure *(Articles 5(1)(f) and 32)*	• Use technical or organisational measures to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage • These measures must be appropriate to the risk, and may include things like: - pseudonymising and encrypting personal data - keep ongoing confidentiality, integrity, availability and resilience of processing systems and services - quick restoration of availability and access to personal data if there is a physical or technical incident - processes for regularly testing, assessing and evaluating security	• If a data breach could have been prevented reasonably easily by the use of appropriate security, this may increase the severity of fines or regulatory enforcement action • Human error often plays a part in data breaches, so building appropriate controls and checks into processes can reduce the risk of accidental or unauthorised disclosure or access • If encrypted devices / media / files are lost or sent to the wrong person and the information is unreadable, this usually won't impact individuals and the breach may not have to be reported to regulators
Make sure you're ready to deal with the enhanced rights for individuals *(Chapter III)*	• Individuals have rights to see a copy of the data you hold on them, to port it, to correct it and to have it deleted, and to object to processing in certain circumstances • Technical and organisational measures need to be implemented to make it easy for people to exercise these rights • People have rights not to be subject to certain automatic decisions or profiling — human intervention / review will need to be built in to these processes	• There is a requirement for subject access requests to be responded to within one month in most cases and, if you don't do this, they can report you to the regulator or take you to court • If you put in place effective systems (e.g. "self-service" preference centres), this can reduce the resources you have to allocate to dealing with requests and can also build trust with individuals
Ensure new products and processes build in "privacy by design" and "privacy by default" *(Article 25)*	• Ensure that new products / processes are built with privacy in mind and that default settings allow for the highest level of protection of personal data	• Considering privacy from the outset (and involving privacy experts early on) will mean that products are built that meet GDPR standards — if privacy is considered too late, this may be more expensive to fix (or even mean that a project has to be called off)

©2018 Centrify Corporation All Rights Reserved.

GDPR requirement	GDPR requirement	Why this is important?
Do Data Protection Impact Assessments (DPIAs) when doing something new **(Article 35)**	• Before starting high risk data processing activities, in particular using new technologies, or involving profiling or high volume sensitive data processing or CCTV in public areas, a DPIA must be carried out • It can be a good idea to do a DPIA even if it is not compulsory	• DPIAs are a key tool to help with risk assessment and involve identifying data protection risks and taking steps to eliminate / minimise these risks • They also can be helpful to present to regulators if there is a problem in the future to show that data protection risks were properly considered
Share people's personal data responsibly *(Article 28 and Chapter VII)*	• Restrict access to personal data internally to people who need to know the information • Only share personal data externally with third parties you trust and are sure can comply with requirements under the GDPR • Put GDPR-compliant data processing contracts in place with all service providers you use to process personal data (and with all customers whose data you process) • Ensure personal data is not transferred outside the European Economic Area unless EU model clauses, Binding Corporate Rules, Privacy Shield or another approved mechanism is used • Ensure people have been properly informed about who their information will be shared with, where and why	• You must make sure that you keep control over information that individuals and customers have entrusted you with and that proper protections are in place with third parties who have access to personal data • When you are processing personal data on behalf of customers, you need to make sure you do not commit to excessive liability / obligations and back off all relevant obligations in contracts with your own suppliers • International data transfers are a particularly high-risk area, particularly when personal data is being transferred to countries that do not have as rigorous data protection laws as in Europe • Think about the "worst case scenario" from the individual's / regulator's perspective — would their privacy be impacted by their information being sent overseas to someone they've never heard of, for reasons they weren't aware of, if there was a data breach?

©2018 Centrify Corporation All Rights Reserved.

GDPR requirement	GDPR requirement	Why this is important?
Be ready to respond to data breaches quickly and effectively *(Articles 33 and 34)*	• Ensure data breaches are quickly detected so you can report to regulators within 72 hours if needed and affected individuals are notified (if required) – this applies if it's electronic data (like the email system) or manual data (like papers in a filing cabinet) • Be able to quickly gather relevant information about the breach for the report to the regulator, including categories and approximate number of affected individuals and records involved; who had access to the data; data protection officer / other contact point's details; likely effect of the breach; measures taken or proposed to address the breach and reduce its impact.	• Breach prevention is always better than "firefighting" • A quick and effective data breach response is key to reducing the potential impact of a data breach • Fines / enforcement action by regulators will be more severe for repeated breaches or if the regulator has previously recommended action and this has not been followed

©2018 Centrify Corporation All Rights Reserved.

How Can Centrify Help

GDPR is not explicit on what controls are needed to mitigate risk in this area — in fact, that may well be a deliberate move designed to future-proof the law as new technologies come and go, and ensure organisations don't resort to a tick-box approach to compliance.

However, it does state that data should be processed in a way that "ensures appropriate security of the personal data, using appropriate technical and organisational measures," taking into account "the state of the art and the costs of implementation." Staying up-to-date with the latest technology advances and following best practice security advice are therefore key to avoiding a damaging breach. Or at least if you are breached they'll help you to avoid follow-on fines for negligence.

So many of these breaches come about because organisations are still reliant on password-based authentication systems. Poor password management makes the attackers' job so easy, allowing them to crack or hack privileged accounts and gain access to your organisation's most sensitive data.

That's why Centrify recommends risk-based multi-factor authentication (MFA), which can decide if a log-in attempt is risky or not and ask for more info from the user if necessary. Combine this with a "least privilege" approach — ensuring staff have no more access to systems, commands and functions than they strictly need — and you'll be off to a great start with GDPR compliance. To learn more, go to www.centrify.com.

Disclaimer

This paper is for information purposes only and the information in this paper does not constitute legal advice. The law changes regularly and this paper sets out the position in September 2017. If you need legal advice on a specific matter, you should consult with a qualified lawyer. To the fullest extent permitted by law, neither Centrify nor Cordery make any representations, warranties, guarantees or undertakings related to the information provided in this paper.

Cordery helps manage the ever-increasing compliance burden. Cordery provides innovative ways of helping General Counsel, compliance professionals and heads of legal across industries manage compliance. Using the expertise of seasoned compliance professionals and the content and technology capabilities of LexisNexis UK we provide expert advice and compliance solutions.

Cordery is licensed by the Solicitors Regulation Authority in the UK as an Alternative Business Structure so that we can provide our solutions and services with the quality, confidentiality and legal privilege that clients value in managing compliance.

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. Centrify's Next-Gen Access is the only industry-recognized solution that uniquely converges Identity-as-a Service (IDaaS), enterprise mobility management (EMM) and privileged access management (PAM). Over 5,000 worldwide organizations, including over half the Fortune 100, trust Centrify to proactively secure their businesses.

US Headquarters +1 (669) 444 5200 | EMEA +44 (0) 1344 317950 | Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876 | Latin America +1 305 900 5354 | sales@centrify.com

Centrify is a registered trademark, and The Breach Stops Here and Next Dimension Security are trademarks of Centrify Corporation. Other trademarks mentioned herein are the property of their respective owners. ©2018 Centrify Corporation. All Rights Reserved.