www.nascenta.com

NASCENTA

Information Security & Resilience

GDPR readiness for start-ups, technology businesses and professional practices

Martin Cassey

NASCENTA
Information Security & Resilience

queries@nascenta.com
01223 926 920

- Introduction
- GDPR – Key Points
- GDPR/DPA Differences
- Start Up, Tech Business Professional Practice?
- Twelve Steps
- Where Can I Get Help?

NASCENTA
Information Security & Resilience

queries@nascenta.com
01223 926 920

Nascenta Ltd

- Private Business - evolution of Cambridge Data Safe Ltd (incorporated 1999)
- Re-launched 2015 as Nascenta Ltd
- Information Security Consultancy & Solutions for SMEs
- People Centric approach – People & Technology

queries@nascenta.com
01223 926 920

Data Protection Legislation

- The UK introduced its first relevant piece of legislation - The Data Protection Act in 1988.
- The GDPR isn't the first foray by the EU into the world of data protection. Directive 95/46/EC was adopted in 1995 and addressed the processing of personal data within the EU.

NASCENTA
Information Security & Resilience
queries@nascenta.com
01223 926 920

Data Protection Enforcement

- **Triforce Recruitment** was fined **£5,000** for failing to notify under section 17 of the Data Protection Act 1998.
- **Whitehead Nursing Group**, was fined **£15,000** for not looking after the sensitive personal details in its care.
- **Regal Chambers Surgery**, was fined **£40,000** after revealing confidential details about a woman and her family.
- **The Money Shop** was fined **£180,000** in response to the loss of computer equipment.
- **Staysure.co.uk Limited**, was fined **£175,000** after more than 5,000 customers had their credit cards used by fraudsters.

NASCENTA
Information Security & Resilience

queries@nascenta.com
01223 926 920

Case Study – Cambs County Council

Cambridgeshire warned to improve data protection

Written by **Colin Marrs** on 11 August 2016 in **News**

publictechnology.net

NASCENTA
Information Security & Resilience
queries@nascenta.com
01223 926 920

Case Study – Cambs County Council

- Deletion of Client records.
- Procedures to review the quality of personal information shared under data sharing agreements (DSAs)
- Checks to provide assurance that retention periods are adhered to.
- Reporting by parties involved in sharing arrangements of any data security incidents or breaches.
- Security Training.

queries@nascenta.com
01223 926 920

Will it happen?…..

- The GDPR takes effect in May 2018. Even under the most optimistic of timetables, the UK will (probably) still be a part of the EU then.
- The Great Repeal Bill will incorporate all existing EU law and regulations, into UK law at the point that the UK leaves the EU.

queries@nascenta.com
01223 926 920

Yes it will!.....

"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."

The Secretary of State Karen Bradley MP, 24 October 2016

'It is right to update our data protection regime not only because we will still be in the EU [at that point], but because it is time to update it, given the enormous changes that have taken place.'

Digital and Culture minister, Matthew Hancock, 12 December 2016

NASCENTA
Information Security & Resilience
queries@nascenta.com
01223 926 920

The EU General Data Protection Regulation

- Although the GDPR entered into force on 25th May 2016, the new rules will only be applied from 25 May 2018.
- That now leaves businesses with less than 18 months to bring their processing activities in line with the new data protection rules.

NASCENTA
Information Security & Resilience

queries@nascenta.com
01223 926 920

7 key principles enshrined in the EU GDPR

1. **lawfulness, fairness and transparency**
2. **purpose limitation**
3. **data minimisation**
4. **accuracy**
5. **storage limitation**
6. **integrity and confidentiality**
7. **accountability**

queries@nascenta.com
01223 926 920

1. **lawfulness, fairness and transparency**
   Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

2. **purpose limitation**
   Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

queries@nascenta.com
01223 926 920

3. **data minimisation**
   Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. **accuracy**
   Personal data shall be 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;

queries@nascenta.com
01223 926 920

5. **storage limitation**

   Personal data shall be 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;

   (Exceptions apply)

queries@nascenta.com
01223 926 920

6. **integrity and confidentiality**
   Personal data shall be 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;

7. **accountability**
   The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1.

queries@nascenta.com
01223 926 920

Additional Restrictions

8. **extra EEA**
   Addresses transfer of personal data which are undergoing processing or are intended for processing after transfer in a third country or to an international organisation.
9. **consent**
   The controller shall be able to demonstrate that the subject has consented.

NASCENTA
Information Security & Resilience
queries@nascenta.com
01223 926 920

Special Categories of Data

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.
- Genetic or biometric data for the purpose of uniquely identifying a person.
- Data concerning health or data concerning a person's sex life or sexual orientation.

Processing of these data types is prohibited, but exceptions do apply.

queries@nascenta.com
01223 926 920

Who doesn't the GDPR apply to?

The GDPR does not apply to certain activities including:

- Processing covered by the Law Enforcement Directive.
- Processing for National Security purposes.
- Processing carried out by Individuals purely for Personal/Household activities..

queries@nascenta.com
01223 926 920

Who does the GDPR apply to?

The GDPR applies to ‘controllers’ and ‘processors’.

- The controller says how and why personal data is processed.
- The processor acts on the controller’s behalf.

queries@nascenta.com
01223 926 920

Data Processors

If you are a processor, the GDPR places specific legal obligations on you; for example:

- You are required to maintain records of personal data and processing activities.
- You will have significantly more legal liability if you are responsible for a breach.

These obligations for processors are a new requirement under the GDPR.

NASCENTA
Information Security & Resilience
queries@nascenta.com
01223 926 920

Data Controllers

If you are a controller, you are not relieved of your obligations where a processor is involved.

The GDPR places further obligations on you to ensure that your contracts with processors comply with the GDPR.

queries@nascenta.com
01223 926 920

DPA 1988 v. GDPR – Some Key Differences

- The GDPR's definition of 'personal data' is more detailed than the DPA. Information such as an IP address, cookie, RFID could be personal data.
- The GDPR applies to manual filing systems where personal data are accessible according to specific criteria. The scope is wider than the DPA and could include chronologically ordered sets of manual records containing personal data.

queries@nascenta.com
01223 926 920

DPA 1988 v. GDPR – Some Key Differences

- GDPR does not include any obligation to register with a regulating body.
- Under the GDPR, consent must be 'freely given, specific and informed' - Silence, pre-ticked boxes or inactivity will not constitute consent.
- The GDPR includes a specific prohibition on the processing of criminal convictions unless permitted by member state law.

queries@nascenta.com
01223 926 920

DPA 1988 v. GDPR – Some Key Differences

- The deadline for compliance Data Subject Access Requests will be one month (rather than 40 days), which can be extendable by a further two months;
- Additional information will need to be provided, such as data retention periods and the right to have inaccurate data corrected.

queries@nascenta.com
01223 926 920

DPA 1988 v. GDPR – Some Key Differences

The GDPR set limits on the use of “profiling” relating to generated computerised data analysis based on the automated processing of his/her personal data.

- Only allowed with the consent of the individual concerned, permitted by law or when needed to pursue a contract and cannot be based solely on automated processing - should comprise human assessment.

queries@nascenta.com
01223 926 920

DPA 1988 v. GDPR – Some Key Differences

- Under the GDPR public authorities and organisations that control large data sets for their core business must designate a Data Protection Officer (DPO).
- A DPO can either be an internal or an external person. The DPO must take responsibility for compliance and have the knowledge, support and authority to do so effectively.

queries@nascenta.com
01223 926 920

DPA 1988 v. GDPR – Some Key Differences

- Breaches have to be reported within 72 hours unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- When there is a high risk from the breach, the controller must communicate the personal data breach to the subject without undue delay.

queries@nascenta.com
01223 926 920

DPA 1988 v. GDPR – Some Key Differences

- Any person who has suffered damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered.
- Breach of the GDPR can result in fines of €20m or, if higher, up to 4% worldwide turnover.

queries@nascenta.com
01223 926 920

Measures

- Pseudonymisation and encryption of personal data;
- Effective back-up;
- Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Regularly testing, assessing and evaluating the effectiveness of security measures;
- Privacy Impact Assessment.

NASCENTA
Information Security & Resilience
queries@nascenta.com
01223 926 920

Start Up/Tech Business/Professional?

- Include GDPR in Business Plan.
- Consider Who, What & Where.
- Secure by Design & Default.
- Competitive Advantage.
- Conduct Privacy Impact Assessment (PIA) if Processing using New Technologies likely to result in a High Risk.

queries@nascenta.com
01223 926 920

Start Up/Tech Business/Professional?

- Data Subject has right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

queries@nascenta.com
01223 926 920

Start Up/Tech Business/Professional?

- Special Consideration for Scientific/Historical Research

  'This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes'

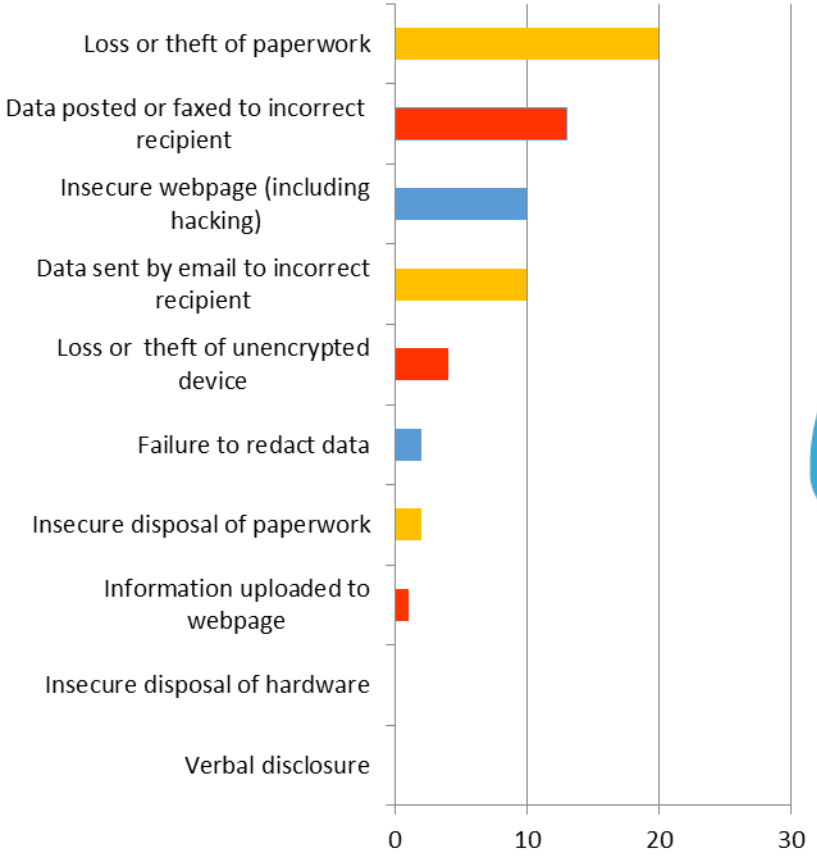
- Consideration of Ethical Standards

  Consent with limits

- Genetic Data included

NASCENTA
Information Security & Resilience
queries@nascenta.com
01223 926 920

Legal sector data security breaches by type in 2015/16



In 2015/16, **4%** of all data security incidents reported to the ICO related to solicitors and barristers.

Data & graphics from ICO

queries@nascenta.com
01223 926 920

Accountants

Elizabeth Denham (head of ICO) delivered a speech to the Institute of Chartered Accountants on 17 January.

She discussed the role of accountability in the GDPR, noting: ‘We’re all going to have to change how we think about data protection.’

queries@nascenta.com
01223 926 920

Accountability

- Accountability pays back - not just in legal compliance, but by providing a competitive edge.

- There is a real opportunity for organisations to present themselves on the basis of how they respect the privacy of individuals and over time this can play more of a role in consumer choice.

queries@nascenta.com
01223 926 920

Compliance

‘Today, many companies think data protection is just about ‘compliance.’ It’s a mindset that says: ‘my job is to meet the legal requirements. As long as I tick the right boxes, we’ll be OK.’

queries@nascenta.com
01223 926 920

Culture

- The GDPR creates an onus on companies to understand the risks that they create for others, and to mitigate those risks.
- Need to move to a mindset of commitment to managing data sensitively and ethically.
- It's about moving to a framework that can be used to build a culture of privacy that pervades the entire organisation.

NASCENTA
Information Security & Resilience

queries@nascenta.com
01223 926 920

Twelve Steps towards GDPR Readiness

1. Raise Awareness across your Organisation and appoint a Senior Information Risk Owner (SIRO)
2. Identify what personal data you hold, where it is, where it came from and who has access to it
3. Review Legal basis for processing data
4. Designate a Data Protection Officer (if needed)
5. If you operate Internationally review what happens where and who regulates your operations
6. Review & update Privacy Notices.

NASCENTA
Information Security & Resilience

queries@nascenta.com
01223 926 920

Twelve Steps towards GDPR Readiness

7. Check ability to comply with Individual's Rights
8. Review how you seek, obtain and record consent
9. Consider if/how you will verify individuals ages and gather parental/guardian consent
10. Update procedures for handling Subject Access Requests.
11. Make sure that you have systems in place to detect, report & investigate personal data breaches
12. Data Protection by Design and PIAs

NASCENTA
Information Security & Resilience

queries@nascenta.com
01223 926 920

Questions?

Martin Cassey
Nascenta Ltd
martin@nascenta.com
+44 (0)1223 926 920