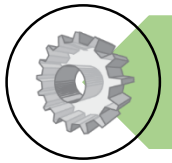
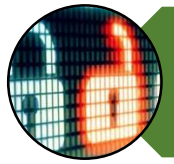
The new General Data Protection Regulation

RADIUS LAW

Law innovated



Privacy must be **designed into** your systems and processes.



New security breach reporting requirements.

Mandatory Data Protection Officers for some businesses.

Extra territorial

Direct accountability for Data Processors

Local adaptions

New expanded consent & privacy notice requirements.

Record levels of complaints to the ICO 14,738 – 50% relate to mishandling of SARS

2017 – Boomerang Video – insufficient website security - £60,000 fine.

2012 – Welcome Financial Services – loss of 2 un-encrypted laptops - £150k fine.

2017 Recruitment Consultant prosecuted for stealing client data

2016 – RSA fined £150k for insufficient security procedures.

2016 - £50,000 fine to GP surgery for mishandling a subject access request.

2012 - Scottish Council fined £250k – employee records in supermarket recycle bin.

2016/17 – ICO crackdown on nuisance calls

2011 Powys Council - £130k fine – Social Worker mistakenly sends data to wrong family because of a shared use of a printer.

2015 Caerphilly Council warned about covert surveillance on an employee

August 2017 – Homes raided – theft of data from car repair centres –sold for nuisance personal injury calls

2014 – MOJ fined £180k – loss of portable drive with sensitive material of 3000 prisoners (no encryption, no password)

2016 – ICO admits it has breached Data Protection Law.

NHS staff prosecuted for accessing patient records.

RADIUS LAW

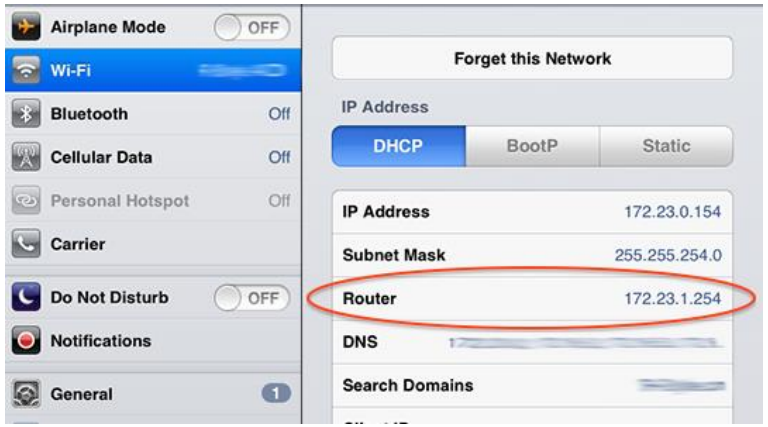
Law innovated

What is Personal Data?

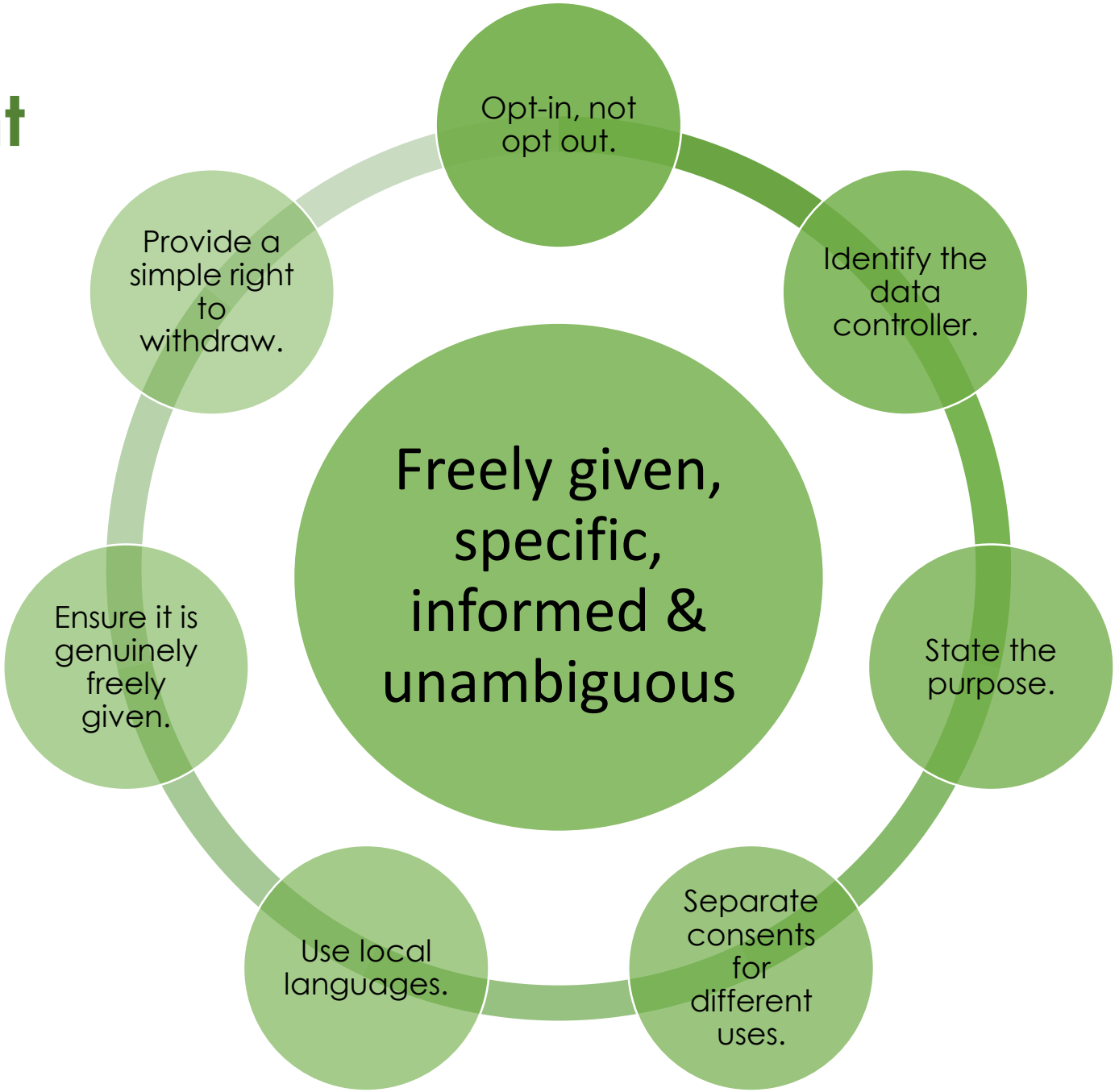
- The Data Protection Act and GDPR concern Personal Data, but what is Personal Data?
- Personal Data is information from which a living individual is identified or identifiable.
- Special category personal data must treated with more caution. Special category personal data includes: racial or ethnic origin, political opinions, trade union membership; physical or mental health, sexual life; commission or alleged commission of an offence. Under GDPR this list is extended to biometric data.

More personal data

- Personal data can include:
  - CCTV;
  - Satellite navigation;
  - On-line identifiers.



Consent



RADIUS LAW

Law innovated

Soft Opt-in

- If an individual has:
  - recently bought something from you; and
  - did not opt-out of marketing; and
  - you gave them clear opportunities to opt out.

  Then you do not need opt-in consent for electronic marketing.
- It's likely that Soft Opt-in will remain under the new E-Privacy Regulation.

RADIUS LAW

Law innovated

Data consents for e-marketing to be GDPR compliant – otherwise must stop

RADIUS LAW

Law innovated

Alternatives to consent

- Consent is just one lawful basis for the processing of personal data. There are alternatives.
  - **Contractual necessity**.
  - Compliance with a legal obligation.
  - Necessary to protect the vital interests of the data subject.
  - Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - **Legitimate interests**.

RADIUS LAW

Law innovated

We need consent, but Help, our database is not GDPR compliant.

Seek GDPR compliant consent

Delete Database

- Seek consent. E-mail campaign (where you have appropriate permission), in-store, outbound phone campaign. Note: Be careful not to contact people that have asked to not be contacted and check Preference Services.
- Delete/ supress database.

RADIUS LAW

Law innovated

Privacy Notices

- Personal data must be collected in a fair open and transparent manner.
- Privacy notices to be **granular**, **concise**, **in local languages**, **transparent**, **intelligible** & **easy to understand.**
- Personal Data must only be used for the purpose that it was obtained.
- Privacy notices must be provided at the time of the data collection (unless exceptions apply).
- ICO recommends a 'layered approach' and the use of innovative formats.
- Privacy notices must include the specified information.

Privacy Notices

What information must be supplied?	Data obtained directly from data subject.	Data not obtained directly from data subject.
Identity & contact details of the Data Controller, the Controller's representative & (where applicable) the Data Protection Officer.	✓	✓
Purpose of the processing and the lawful basis for the processing.	✓	✓
The legitimate interests of the controller or third party, where applicable.	✓	✓
Categories of personal data.		✓
Any recipient or categories of recipients of the personal data.	✓	✓
Details of transfers to third country (Countries outside of the EU) and safeguards.	✓	✓
Retention period or criteria used to determine the retention period.	✓	✓

RADIUS LAW

Law innovated

Privacy Notices

What information must be supplied?	Data obtained directly from data subject.	Data not obtained directly from data subject.
The existence of each of data subject's rights.	✓	✓
The right to withdraw consent at any time (where relevant).	✓	✓
The right to lodge a complaint with a supervisory authority.	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources.		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

RADIUS LAW

Law innovated

B2B and B2C

Communication Method	Business to Consumers (including sole traders and partnerships)	Business to Business
Live calls	• Screen against TPS. • Can opt out.	• Screen against Corporate TPS. • Can opt out.
Recorded Calls	• Need specific consent.	• Need specific consent.
Emails or texts	• Need specific consent or soft opt-in.	• Can email or text companies. • Individuals can opt out.
Faxes	• Need specific consent.	• Screen against FPS. • Can opt out.
Mail	• Name & address obtained fairly. • Can opt out. • Recommend – check against MPS	• Can mail companies. • Individuals can opt out.

RADIUS LAW

Law innovated

Data Processors

- Data Processors will have some direct responsibility under GDPR. Data Controllers still responsible for Data Processors
- GDPR mandates some provisions in all Data Controller to Data Processor contracts.
- Data Controllers are likely to undertake more due diligence on Data Processors.
- Data standards such as ISO27001 and PCI-DSS will be more important.
- Contracts must be future-proofed against GDPR and Brexit

Rights of Individuals

- A SAR is a right for individuals to obtain personal data from a Data Controller that it holds about them, why it is held and who it is disclosed to.
- A SAR does not have to be in any specific format – so important that staff identify a SAR and react quickly.
- 50% of ICO complaints relate to mishandling of SARS.
- A new Code of Practice was issued by the ICO in mid 2017 – but not yet updated for GDPR.
- Information to be provided:
  - told whether any personal data is being processed;
  - given a description of the personal data, the reasons it is being processed, and whether it has been/ will be given to other organisations;
  - given a copy of the personal data; and
  - given details of the source of the data (where this is available).

RADIUS LAW

Law innovated

Rights of individuals

- There are some exceptions to the data that must be released:
  - Confidential references given;
  - Data that's processed for the prevention or detection of crime;
  - Management information that would prejudice the business of the organisation;
  - Records of negotiations;
  - Legal advice.
- Subject access requests (continued)
  - No fee Under GDPR.
  - Response must be within 1 month (reduced from 40 days).
  - Right to ask reasonable questions/ ID checks.
  - Carefully consider the release of data relating to another person in the SAR response. Seek consent where appropriate. In some cases it will be necessary to redact other personal data.

RADIUS LAW

Law innovated

Rights of Individuals

- Right to be forgotten.
- Right to restrict the data.
- Right to correct the data.
- Right to withdraw consent/ object to processing.
  - Supress, don't delete.
  - Notify right to withdraw consent
  - Withdrawal of consent must be simple and automated if on-line.
- Right to have data ported to a new provider (subject to some exceptions).
- Right to restrict profiling.
- Right to complain to authorities, right to remedies and right to compensation.

RADIUS LAW

Law innovated

Security & Standards

- Only collect the data that you need.
- Data must be accurate and up to date.
- Only keep data for as long as you need it. Define and enforce retention policies.
- Manage the data appropriately:
  - Privacy by Design and Privacy Impact Assessments;
  - Use pseudonymisation where possible;
  - Don't use a 'one size fits all' approach;
  - Evidence compliance.
- Staff training is a base-line expectation for all organisations that handle personal data.
- BYOD (Bring your own Device) – Refer to ICO specific guidance.

RADIUS LAW

Law innovated

Security & Standards

- Appropriate technical & organisational measures to guard against unlawful processing.
  - Where is your data stored?
  - Is it secure? Think about both hard copy and electronic records.
- Data Breach reporting (from GDPR day)
  - Notify breaches to the regulator.
  - Data Processors must report to Controllers - without undue delay after becoming aware of it. Data Controllers must report to supervisory authorities – without undue delay and w/n 72 hours of becoming aware of it.
  - A data breach is '*accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data*'
  - BUT no reporting is necessary if breach is unlikely to result in a risk to the rights and freedoms of natural persons. (Note: no exceptions for Data Processors)
  - Supervisory authority may compel a report to subjects.
  - Implement a breach response plan. **Containment & Recovery**, **Assessment of Risk**, **Notification**, **Response**.
  - Must maintain a breach register.
- Right to release data in certain circumstances – prevention and detection of crime.

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

Data Protection Officers

- GDPR requires DPO's to be appointed – for:
  - Public authorities;
  - Any organisation whose core activities require:
    - *'regular and systematic monitoring'* of data subjects *'on a large scale'* or
    - *'large scale'* processing of Sensitive Data or criminal records.
  - those required to do so by local law (e.g. Germany)
- If an organisation determines it does not need to appoint a DPO it must document why.

RADIUS LAW

Law innovated

Transferring data outside of the EEA

- Generally, personal data must not be transferred outside of the EEA. There are some permitted exceptions, including:
  - where the data is transferred to a country approved by European Commission (to have adequate security);
  - explicit consent by the data subject;
  - there is a 'commission approved' contract with the other party;
  - the data is transferred within group company offices that have approved binding corporate rules in place;
  - there is a certified mechanism e.g. EU US Privacy Shield.

RADIUS LAW

Law innovated

Employees

- Contract terms
- Policies
- Restrictive covenants
- Training
- Don’t forget temps and contractors
- Monitoring

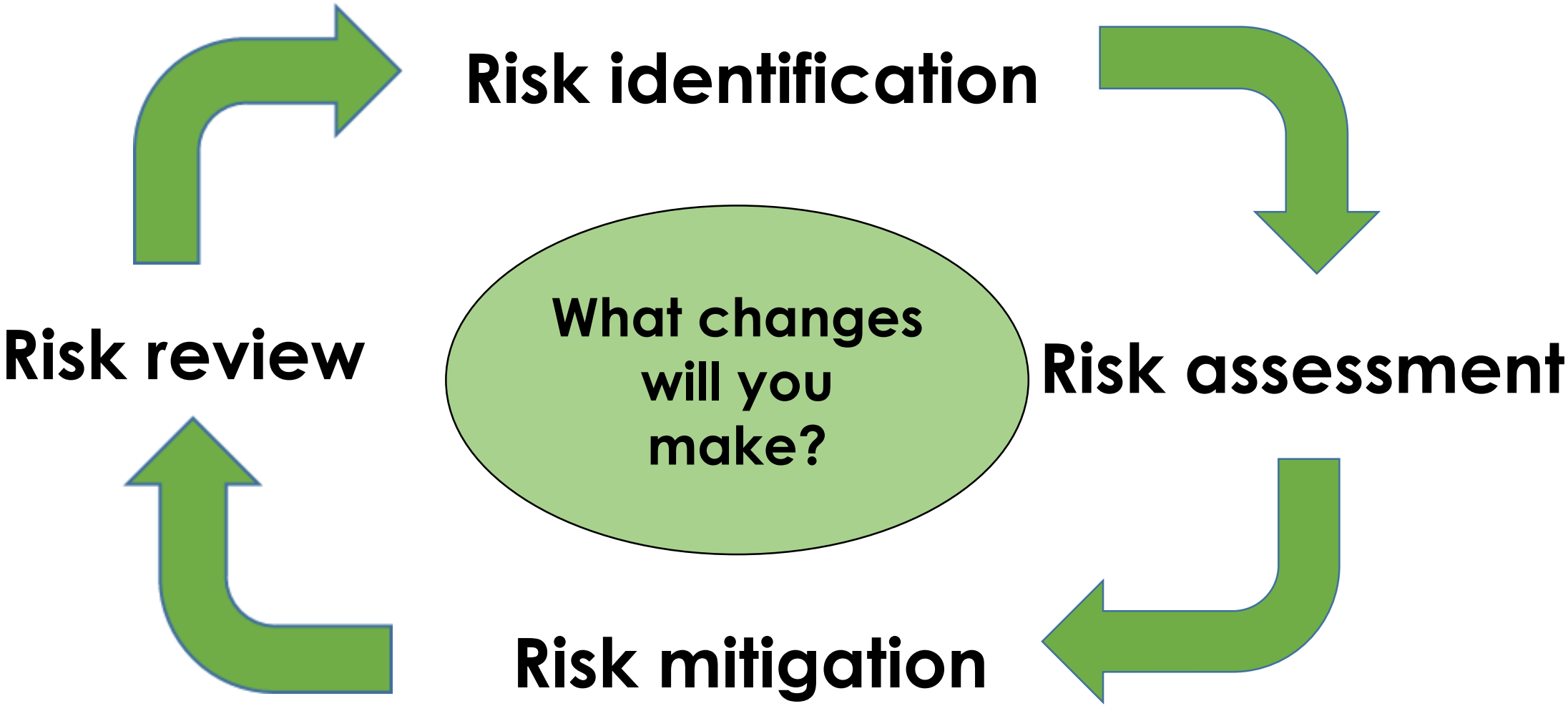
RADIUS LAW

Law innovated

Recommended policies & documentation

- Data Protection Policy;
- Privacy Policies (Customers, Staff, Website);
- Consent Notices;
- Home Working Policy;
- IT Security and BYOD Policy;
- Subject access policy;
- Monitoring policy;
- Social Media Policy;
- Data Breach Response Policy;
- Employment contracts;
- Controller-Processor contracts.

RADIUS LAW
Law innovated



RADIUS LAW
Law innovated

Next Steps

- Confirm GDPR Lead within your Centre
- Review GDPR Checklist and assess gaps with current condition
- Identify counter measure actions to address gaps and document against Checklist
- Begin process of validating Customer Consent data (active customers only)
- Review Customer Database to ensure only ‘Legitimate’ customer records are being held
- Work towards Q1 2018 for interim review of GDPR readiness
- Review current Data Privacy Policies and Fair Collection Notice – refer to example provided by TGB
- Any questions please refer to Phong Tran (TGB) : phong.tran@tgb.toyota.co.uk

TOYOTA

ALWAYS A BETTER WAY

Further information

- Information Commissioner's Office (ICO) – includes access to newsletters and conferences www.ico.org.uk
- Cyber Essentials https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
- EU Data Protection (Article 29 Working Party) - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- Get Safe On-line www.gestsafeonline.org
- Business Link - www.businesslink.gov.uk
- Fraud Advisory Panel - www.fraudadvisorypanel.org/

RADIUS LAW

Law innovated

GDPR is coming.

Is your business ready?

WHAT IS GDPR?

- The new General Data Protection Regulation (GDPR) will become law on the **25th May 2018.**
- The GDPR is the most significant change to Data Protection Law in 20 years.

WHAT'S CHANGING?

Lots - here are the headline changes:

New expanded consent requirements. *You may need to stop marketing activity if your prospect database is not 'GDPR compliant'.*

Privacy must be **designed into** your systems and processes.

New security breach reporting requirements.

Mandatory Data Protection Officers for some businesses.

The fines are going up. Pre-2010 the max fines were £5,000. In May 2018 **max fines increase to the higher of €20m/ 4% turn-over.**

IS THIS RELEVANT TO AUTOMOTIVE?

Yes, like many businesses, customer data is core to the operation and value of the business. The data held often contains payment information which increases the profile and risk. One motor manufacturer has already been fined by the Data Regulator for making mistakes with its GDPR programme.

DO I NEED TO TAKE ACTION NOW?

The GDPR is effective from 25th May 2018. It's important that preparations start now to prepare for the new regime. This will help to ensure current marketing activities can continue and to minimise the risk of regulator action.

WHAT SHOULD I DO?

We have created an Automotive GDPR Readiness Check (more details overleaf). This is designed to identify gaps in compliance and provide recommendations for fixes.

WHY RADIUS?

- Radius is a specialist automotive law firm so intuitively knows about the data risks.
- Radius has significant experience in data security and has designed its own bespoke programme.
- We only engage senior lawyers – who are expert in providing practical legal solutions.
- Our innovative business model keeps our costs and fees low.

ENDORSED BY

THE MOTOR OMBUDSMAN

THE MOTOR CYCLE INDUSTRY ASSOCIATION

GDPR Automotive

Readiness Check Options

LITE

- Structured telephone interview.
- GDPR Readiness Report – GAP analysis & recommendations.

£1,500 (plus VAT)

COMMERCIAL

- On-site (1 UK location, 1 day);
- 1.5 hour training presentation;
- Structured interview x 2;
- Review of 3 sample policies and 2 sample contracts;
- GDPR Readiness Report – GAP analysis & recommendations.

£3,500 (plus VAT & expenses)

BESPOKE

- Just want it sorted? – We can complete the GDPR Readiness Report and implement all remedial actions.
- We will need some time with you to understand scope – but then happy to provide a fixed fee.

£POA

COLLABOR8™

- 4 x in-person training & co-ordination half days;
- 1.5 hour training presentation at kick-off event;
- Review of 5 sample policies and contracts (across Collabor8 Group – not per member);
- 1 structured telephone interview - each Collabor8 Group member;
- GDPR Readiness Report – GAP analysis & recommendations

Collabor8 is a cost share idea. You organise a venue and other businesses to join the Collabor8 group (8 members). Collabor8 allows time for in-person meetings, more content than Lite & the opportunity to share and learn with other businesses.

£2,000 per member (plus VAT & expenses)

WHAT'S INCLUDED?

Our Data Security Readiness check will analyse your business practices against the new GDPR Requirements and produce a scored report identifying areas of non-compliance and recommendations for solutions.

WHAT'S EXCLUDED?

The Readiness Check will not include work that may result from the recommendations (unless you have selected Bespoke). The report may, for example, identify that the Information Notices are deficient because they do not include the identity of the data controllers. It will not provide a revised Information Notice.

WHAT NEXT?

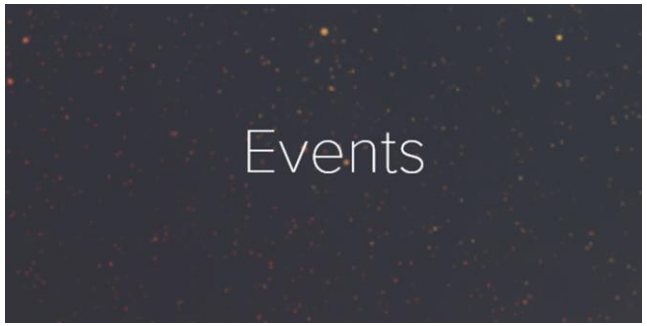
For more information or to book your Readiness Check please contact us on:

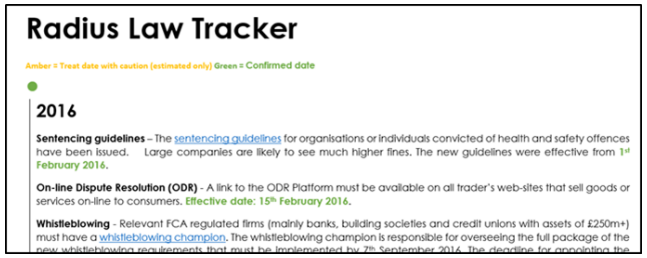
01727 808503
office@radiuslaw.co.uk

RADIUS LAW

RADIUS LAW

Law innovated




Radius Law Tracker

Amber = Treat date with caution (estimated only) Green = Confirmed date

2016

Sentencing guidelines – The sentencing guidelines for organisations or individuals convicted of health and safety offences have been issued. Large companies are likely to see much higher fines. The new guidelines were effective from 1st February 2016.

On-line Dispute Resolution (ODR) - A link to the ODR Platform must be available on all trader's web-sites that sell goods or services on-line to consumers. Effective date: 15th February 2016.

Whistleblowing - Relevant FCA regulated firms (mainly banks, building societies and credit unions with assets of £250m+) must have a whistleblowing champion. The whistleblowing champion is responsible for overseeing the full package of the

Radius Law

keeping you up to date

Iain Larkins, Director
Radius Law Limited
5 The Old Dairy Mews
Caste Road
St Albans AL1 5FJ

01727 808503
07767 886253
iain.larkins@radiuslaw.co.uk
www.radiuslaw.co.uk

RADIUS LAW

Law innovated