Who are Silver Jet?

SILVERJET INSIGHT is here to improve customer experiences and grow loyalty through developing a deep understanding of your customer behaviour

Intelligent marketing using a data driven approach

We have a passion for data driven marketing, making intelligent decisions that drives results, focusing on ROI

Our experience covers all areas of marketing, with a specialism in marketing analytics, CRM, direct communications, telesales, segmentations and customer journeys

GDPR

Promoting your business in a GDPR (General Data Protection Regulations) world

Stephen James

SILVERJET INSIGHT

DATA DRIVEN DECISION MAKING

GDPR

The contents of this presentation should not be interpreted as legal advice. Consult your legal counsel if you are unsure if your actions would be compliant.

Why should you listen to me?

Over the years we have sent millions and millions of communications to millions of people, where being on the ball with legal compliance is a necessity

Complaints from organisations such as ICO and TPS averaged around 1 per year, showing a great understanding for the legal requirements and how to make best use of direct communications

What does GDPR aim to do?

From a sales and marketing perspective the starting point for understanding what GDPR means for you is Article 5

Article 5 of the GDPR sets out the requirements for personal data, across 6 clauses, containing lots of text and legal language

But simply:

Its about transparency and accountability therefore:

Giving data proper respect

What about PECR?

While GDPR has all the headlines, just as critical is PECR

Privacy and Electronic Communications Regulations (ePrivacy Directive)

If you:

- Market by phone, email, text or fax
- Use cookies or a similar technology on your website
- Compile a telephone directory (or a similar public directory)

PECR applies to you

What about PECR?

- Key requirement of PECR is consent
- Individuals must be informed as to what they and have been given
- You must have consent to process data under PECR

What about PECR?

You should keep records of what a person has consented to, and when and how you got this consent

Your audit records will be essential to demonstrating compliance in the event of a complaint

You should be very careful when relying on indirect consent (consent originally given to a third party)

- You must make checks to ensure that the consent is valid and specifically covers your marketing
- Generic consent covering any third party is unlikely to be enough

What does GDPR aim to do?

Can I be fined 4% of my annual turnover?

Yes, 4% of annual global turnover or €20m, whichever is smaller

There is a lower level of 2% of annual global turnover or €10m, whichever is smaller, for less serious infractions

But before you panic, here's what the ICO's information Commissioner has to say…

What does GDPR aim to do?

Taken from the Information commissioners blog, ICO blog: GDPR - sorting the fact from the fiction,

“the biggest threat to organisations is not massive fines, it is harming your own reputation”

“This law is about putting the consumer and citizens first”

“It is scaremongering to say the ICO will be making early examples of organisations for minor infractions or massive fines will be the norm”

“Last year (2016/2017) we concluded 17,300 cases. 16 of them resulted in fines”

“We intend to use those powers proportionately and judiciously”

Based on their track record, the ICO will not be looking to come down hard on businesses that make mistakes in trying to comply with the GDPR

As ever, it is organisations that take liberties with data that should be worried

Personal data

Personal data is the foundation of the new regulations, you need to understand:

- What it is
- Whose it is
- How you use it
- The data owners rights

Personal data

GDPR and other data protection laws rely on the term 'personal data'

There are two key types of personal data in the UK

Personal data

- Personal data can be anything that allows a living person to be directly or indirectly identified. This may be a name, an address, an IP address or even automated personal data if a person can be identified from it

Sensitive personal data

- GDPR calls sensitive personal data as being in 'special categories' of information. These include trade union membership, religious beliefs, political opinions, racial information, and sexual orientation

Personal data

When it comes to collecting data:

If you don't need it, don’t collect it

To be clear there is no distinction between personal data about individuals in their private, public or work roles

The person is the person

If you hold a person’s data on your systems, you are the custodian of that data, not the owner

Data is always owned by the Data Subject

Personal data

Individuals need to know what they are signing up for, be clear, be explicit about how you will use their personal data

- Communications
- Profiling
- Other Group organisations
- Third parties

Personal data

People have more rights under GDPR

- Right to be informed - about how, why and where your data is used. It is the controller's responsibility to inform you by request.
- Right to be forgotten - If you want your data to be deleted from any server or data storage, even if you have previously given consent, you can have it deleted.
- Right of rectification and restriction - You can have your data corrected at all times if any information about you appears to be inaccurate or incomplete. You can also request a limitation to the access and handling of your data.
- Right to object - if you have been automatically profiled. You also have the right to object if it affects you significantly. Furthermore, you can object to direct marketing.
- Right to portability - If you are unhappy with the way your data has been treated, it is possible for you to move your data to another controller.
- Right to complain - As you are the data owner, the regulation aims at protecting you when companies or third parties infringe your rights.

Controllers, processors & officers

There are 3 roles that are key in understanding your GDPR responsibilities and understanding the role that you play in your organisation

Controllers

- The entity that determines the purposes, conditions and means of the processing of personal data
- This can be a person or an organisation
- You are not relieved of your obligations where a processor is involved

Controllers, processors & officers

There are 3 roles that are key in understanding your GDPR responsibilities and understanding the role that you play in your organisation

Processors

- The entity that processes data on behalf of the Data Controller
- You will have internal processors and may have external processors
- If you are a processor, the GDPR places specific legal obligations on you
  - you are required to maintain records of personal data and processing activities
  - You will have legal liability if you are responsible for a breach

Controllers, processors & officers

There are 3 roles that are key in understanding your GDPR responsibilities and understanding the role that you play in your organisation

Data Protection officers

Should be an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Legislation defines the DPO's tasks as:

- To inform and advise the organisation and its employees about their compliance obligations
- To monitor the organisations compliance
- To be the first point of contact for supervisory authorities and for individuals whose data is processed

Controllers, processors & officers

Under the GDPR, you must appoint a DPO if you:

- Are a public authority (except for courts acting in their judicial capacity)
- Carry out large scale systematic monitoring of individuals (for example, online behaviour tracking)
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offences

Large organisations should look to appoint a DPO regardless of these requirements as it would be best practice

We suggest that when looking for someone to fulfil the DPO role, start with the person that has the most interaction with your customer data as they are likely to be the most suitable

International data transfer

Personal data may only be transferred outside of the EU in compliance with the GDPR

There needs to be:

- A legally binding agreement between public authorities or bodies
- Binding corporate agreements
- Compliance with an approved code of conduct

You are responsible for carrying out your own due diligence and ensuring that your suppliers/service providers meet these requirements

A safety first approach would be to look at UK/EU based suppliers as they are legally bound to comply with GDPR

Privacy information

A privacy notice/policy must tell people:

- Who you are
- What you are going to do with their information
- Who it will be shared with

These are the basics upon which all privacy notices should be built

They can also tell people more than and should do so where not telling people will make your processing of that information unfair

It is good practice to use the same medium you use to collect personal information to deliver privacy notices e.g. if you collect the data online, you should have your privacy policy on the data collection page

Privacy information

You may decide it is beneficial to go beyond the basics, for example by telling people:

- The different types of data you collect and the purposes for them
- The consequences of not providing information
- What you are doing to ensure the security of personal information
- Information about their rights of access to their data
- What you will not do with their data

This level of disclosure goes above the minimum legal requirements

It takes the spirit of the law much further, a truly open approach to your customers privacy

Privacy information

A great example of a clear, concise and engaging privacy notice:

Channel 4 viewer promise

We live by three rules when it comes to Privacy Notices:

- Say what you'll do
- Do what you say
- Don't surprise anybody

Consent

The requirements surrounding consent is one of the leading subjects in the GDPR

Article 4(11) of the GDPR stipulates that consent of the data subject means it is:

- Freely given
- Specific
- Informed
- Unambiguous

Consent

Freely given

Consent is considered to be freely given if:

- It isn’t bundled up in terms & conditions
- If the data subject doesn’t feel compelled or coerced into giving it
- If the data subject can remove consent without it being detrimental to them

Consent

Specific

This aims to ensure transparency and that the data subject has a degree of control

Consent must be in relation to specific purposes

Consent

Informed

This is part of the fundamental principle of GDPR, transparency, lawfulness and fairness

You need to provide information to data subjects prior to obtaining their consent, enabling them to make informed decisions

If you do not provide accessible information consent will be invalid

Consent

Unambiguous

Consent requires a statement or a clear, deliberate affirmative act

Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action

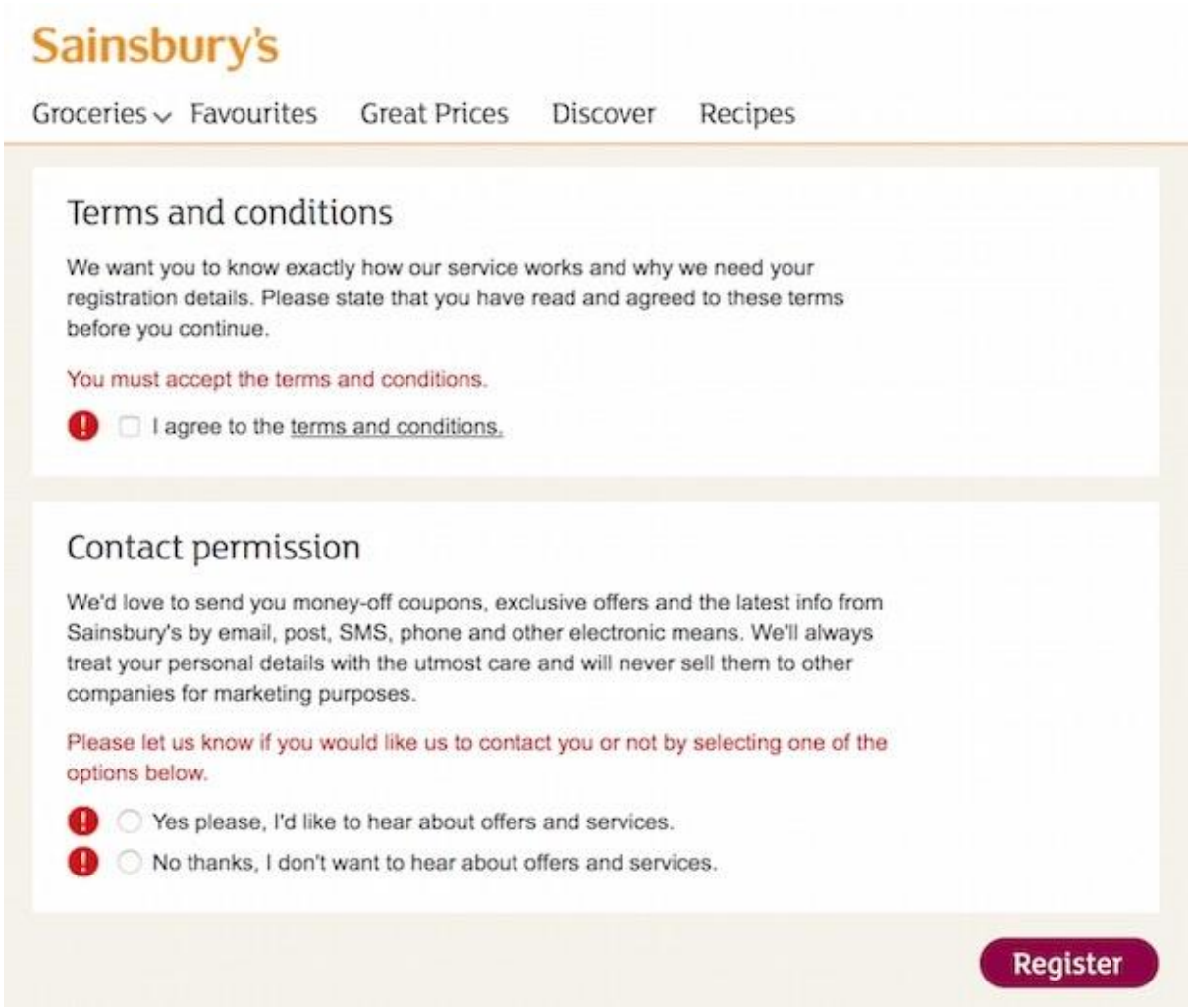
Pre-ticked boxes or opt-out constructions that require an intervention from the data subject (for example ‘opt-out boxes’) are not allowed

Consent

There is no specific time limit for how long consent lasts

Time limit depends on the context, the scope of the original consent and the expectations of the data subject

If the processing operations change or evolve considerably then the original consent is no longer valid



Consent Best Practice Example

Unbundled consent
Separating marketing consent from the Terms & Conditions

Marketing consent sits separately to the Terms and conditions that apply to the service being provided

Sainsbury's

Consent Best Practice Example

Keep in touch with us

Please tick the boxes below to tell us all the ways you would prefer to hear from us:

- ☐ Yes please, I would like to receive communications by email
- ☐ Yes please, I would like to receive communications by telephone
- ☐ Yes please, I would like to receive communications by mobile (text message)
- ☐ No thank you, I **do not** wish to receive communications by post

Granular consent
Separating channel consent

Consent has been broken down for the user to opt into each channel

The ‘post’ opt is not the absolute best practice, but is likely to be the most common application of consent as it leaves the door open for direct mail marketing under Legitimate Interests

Consent Best Practice Example

Here at [organisation name] we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

Post ☐ **Email** ☐ **Telephone** ☐

Text message ☐ **Automated call** ☐

We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:

I agree ☐

There is no reason why you couldn't take the granular approach further and gain opt in for different types of communications, e.g. product offers, industry information, but be aware of click fatigue and the possibility that customers may skip it all together

Granular consent
Separating channel consent

This is from the ICO, the body responsible for enforcing GDPR in the UK

If you want the most comprehensive and lowest risk approach to data collection and usage, this is the template to follow

ico.
Information Commissioner's Office

Consent Best Practice Example

At Waitrose, we have exciting offers and news about our products and services that we hope you'd like to hear about. By providing your details you agree to be contacted by us*. We will treat your data with respect and you can find the details in our Contact Promise.

If you would prefer not to hear from us, you can stop receiving our updates at any time by getting in touch or by letting us know below.

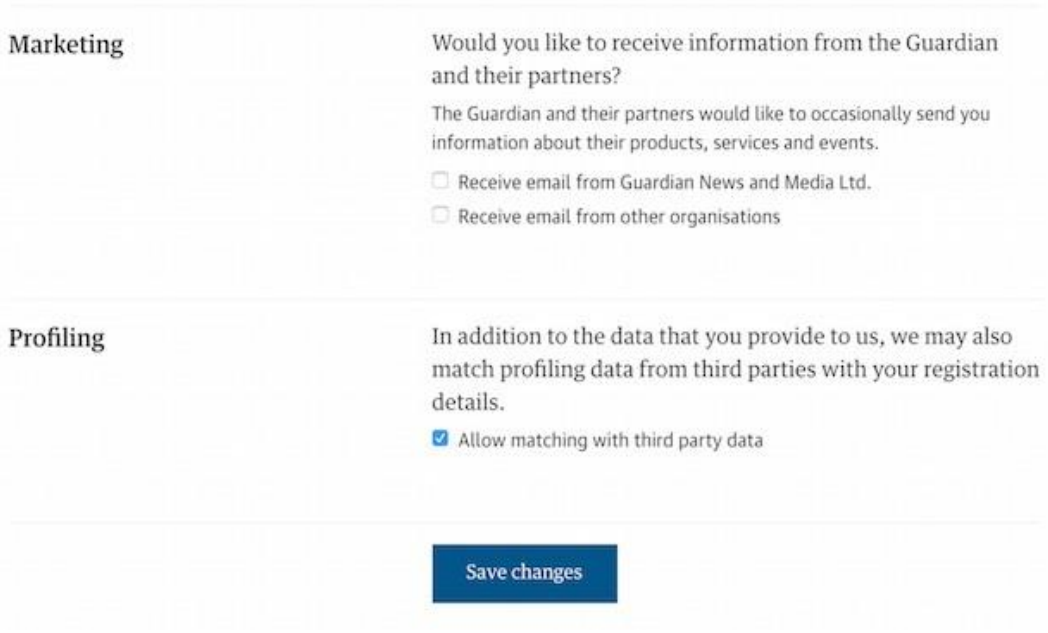
- I'd prefer **not** to receive updates from Waitrose
- I'd prefer **not** to receive updates from John Lewis
- I'd prefer **not** to receive updates from John Lewis Financial Services

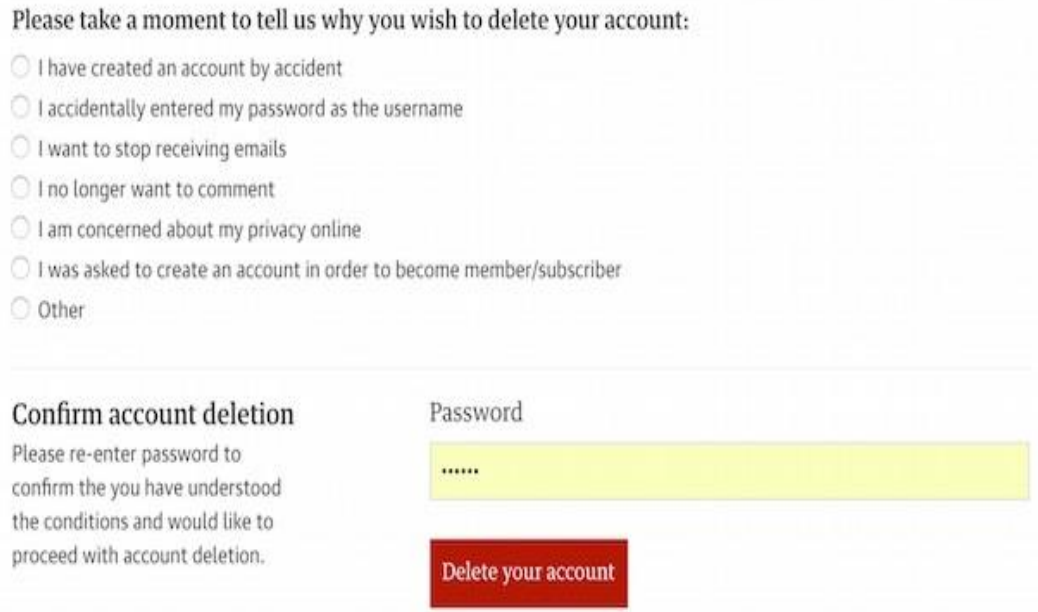
Named organisations
Separating consent to be contacted by organisations within a group

Enables subjects to choose which, if any, businesses in a group to be contacted by

Waitrose

Consent Best Practice Example





Withdrawal/Erasure

The top example shows the ability to remove consent to profiling using external data

The bottom example shows the ease in which the right to be forgotten can be exercised. The webpage also states: "Deleting your account removes personal information from our database. Your email address becomes permanently reserved and the same email address cannot be re-used to register a new account."

the guardian

Consent

Re-consenting

The belt and braces approach:

If you cannot prove that consent was gained to GDPR standards then it is not considered as an opt in, you need to get it again

Only look to re-consent those who have previously given consent to you

Do not ask individuals for consent if they have already opted out

Consent

Re-consenting

Bringing GDPR and PECR together gives another view

If you collect consent with a soft opt-in then you can continue to use this as a legal basis for marketing under legitimate interests

A soft opt-in describes the rule about existing customers

The idea is that if an individual bought something from you recently, gave you their details, and did not opt out of marketing messages, they are probably happy to receive marketing from you about similar products or services even if they haven’t specifically consented

You must have given a clear chance to opt out when you first collected their details

You must give a chance to opt out in every message you send

The soft opt-in rule means you may be able to email or text your own customers, but it does not apply to prospective customers or new contacts

Legitimate Interests

Legitimate Interests is the most flexible lawful basis for processing data, but not always the most appropriate

Relying on Legitimate Interests means you take on extra responsibility for ensuring people's rights and interests are fully considered and protected

You can rely on Legitimate Interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object - and if you don't need consent under PECR

To use Legitimate Interests, a LIA (Legitimate Interests Assessment) must be completed to establish if there is an acceptable balance between the interests of the controller and the rights and freedoms of the individual

Here is a useful document for understanding and using Legitimate Interests: Data Protection Network - Legitimate Interests guidance and Assessment template

Consent v Legitimate Interests

Consent

- Crystal clear permission from the subject
- People know exactly what to expect
- Doesn’t last forever
- If withdrawn, you have to act without delay
- Requires a positive action, which is harder to get
- You can only do what you said at the time you collected the consent

Legitimate Interests

- Far more flexible as a basis for processing
- Increases scope for usage
- Enables the use of some legacy data
- LIAs can be time consuming to complete
- LIAs must be kept in case of a complaint
- LIAs are subjective, your opinion might not be that of the governing body

Consent v Legitimate Interests

Consent vs Legitimate Interests

Each legal basis for processing has its benefits

- Consent carries the least risk
- Legitimate Interests has more risk, but has greater scope for use

Over coming weeks you will probably notice many large organisations informing you about their intention to use Legitimate Interests as their basis for processing your data

This may give you an idea about the method generally preferred by the sales and marketing industry

If you choose to process data under consent, you cannot change to using Legitimate Interests

What else is essential to know about GDPR?

Non marketing business communications

Consent rules do not apply where communications relate to the transactional nature of doing business:

- Service interruptions
- Delivery arrangements
- Product safety
- Changes to terms and conditions
- Store location changes
- Contact changes (account phone number)

If they contain a sales or marketing message of any form, they are considered to be marketing communications

Non marketing communications will probably become more common in the future

They would represent an opportunity to communicate with a customer. You won't be able to use promotional terminology, but you would still be getting yourself in front of a customer, putting you at the front of mind

The opportunity in GDPR

Carry out a data audit

Know who you can contact legally

Understand the ways that you process data

Know the basis on which you will be operating

- Consent
- Legitimate interests

This is your starting point, do this and you know:

- Who you can contact
- Using which channels
- Under which legal basis

The opportunity in GDPR

- Better quality database
- Only talk to those that want to hear from you
- Reduces wastage/cost
- Increases campaign effectiveness and Return On Investment
- Enables you to better focus your resources

The opportunity in GDPR

Be more relevant

Target the message to the customer

Use personalisation to engage the customer

Show your customers that by having access to their data you are improving their customer experience

Targeted and personalised message have a track record of making incremental improvements to marketing activity, generating more responses, greater sales and greater profits

The opportunity in GDPR

Brand perception

Show you are doing the right things for your customers

New customers will see how you value them and their privacy

Shows how the customer is central to what you do

- Make them feel more valued
- They trust you more
- You have a greater reputation

Your brand perception is part of your overall value proposition, playing a part in your ability to attract customers, engage them and generate great returns

The opportunity in GDPR

Manage your customer journey

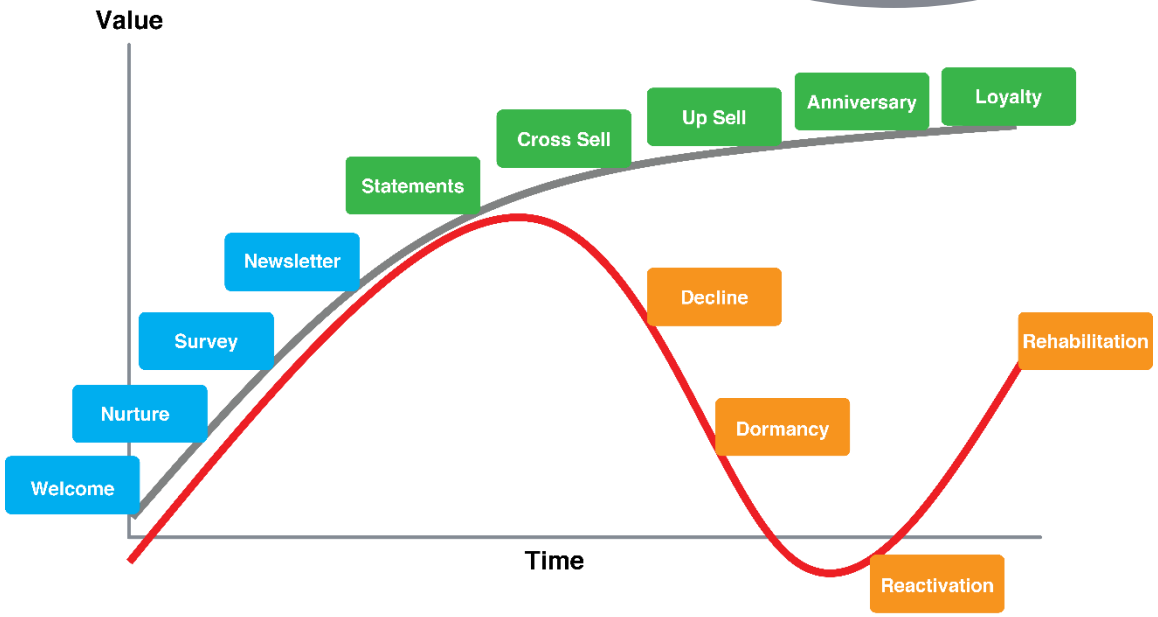
If you have consent, they want to hear from you

If you are using legitimate interests, timely communications will do wonders

Communicate regularly with good content

Show your customers that you value them and use their data appropriately

Use a managed customer journey to build on your existing relationships, using great marketing to support the rest of your business and add revenue



The opportunity in GDPR

Summary

GDPR shouldn’t be viewed as a box ticking exercise, it is an opportunity

If your competitors see it as a legal burden, their customers will see through them

Behind every email address, phone number, post box; is a person

Treat their data with the same respect as you would treat them

It will pay dividends