

PART 1

# Consent must be freely given and data cannot be excessive



**GDPR ensures that a Data Subject is able to give consent to their personal data by ensuring that the request is made in an easily understandable way.**

As such, a data subject will have the right to give and withdraw consent but must have understood clearly what data they were being asked for and why and what will it be processed for, so that they can themselves accept to give the data and make an informed decision if they deem the request is valid or not and in no way excessive.

In this regard companies will no longer be able to use long winded legalise to obscure the reasons why data is given. Requests for consent must be given in an intelligible and easily accessible form, with the exact purpose for data processing attached to that consent.

- > Consent must be unambiguous.
- > Consent must be clear and distinguishable from other matters
- > Consent must be provided in an intelligible and easily accessible form, using clear and plain language.
- > Consent must be as easy to withdraw, as it is to give it.
- > Proof of consent must be kept.

**For non-sensitive data, "unambiguous" consent will suffice.**

**Explicit consent is required only for processing sensitive personal data, so only an explicit "opt in" will suffice.**

## Direct Marketing

If a data subject appears on a list obtained you must notify the Data Subject within 30 days and remove them if requested. When seeking consent you should ask consent for every process you will perform on the data as consent could be withdrawn. You could end up having an email address consented to email invoices, support notification but restricted from direct marketing. Are you system ready for this multi choice option?

## ✓ Action Points

Commence a thorough review of your organisation and ensure all the data you have on a data subject has been consented to for each process performed.

Review all personally identifiable data and ensure it was obtained freely.

Ensure the data was needed for the purpose outlined and was not excessive in its nature.

Seek consent if unsure and immediately stop processing the personally identifiable data if the purpose was not consented to.

Ensure the consent is recorded so it can be proved at a later date is required.

PART 2

# Fair and Lawful Processing of data



GDPR ensures that all the data you have on a data subject must be:

- > Processed lawfully.
- > Collected for the explicit lawful purposes only.
- > Processing is adequate and relevant but limited to what is necessary for as in the purpose it was provided for.
- > The data you hold must be kept accurate and kept up to date.
- > Data must be kept in a form that makes it easy to identify when no longer needed.
- > Data must be processed in a way that ensures appropriate security of personal data.
- > Data Consented can also be withdrawn.

## ✓ Action Points

Ensure all your data is up to date and accurate as it is your responsibility.

No more pre ticked boxes. Consent must have been given freely and easy to have been understood.

Make sure to remove any inaccurate data or data you have no lawful purpose to have.

Ensure to look at your data and see what you no longer need and how easy it is to access.

Make sure the processing of the data when it comes to personal data has adequate security measure in force.

Conduct regular audits on systems that have Personally Identifiable Data to ensure you are still compliant.

## PART 3

# Purpose Limitation



**Personal Identifiable Data relating to a Data subject must be obtained fairly according to the purpose that was outlined when it was obtained. Personal data shall be processed lawfully and fairly and in a transparent manner in relation to the data subject.**

Personal Identifiable Data can only be used for the reasons you informed the person you needed it for and the exact purpose you told the data subject you needed it for. So its use must be limited.

Ensure that if the data is being shared with other parties that consent has been freely given and if so that processing is fair and lawful. If not seek consent and if not given stop.

## USEFUL DEFINITIONS

### Article 4 GDPR:

- > **Data Subject** is defined as any information relating to an identifiable natural person.
- > **Personal Data** means any information relating to an identified or identifiable natural person.
- > **Controller** means the natural or legal person, public authority, agency or other body which alone or jointly with other determines the purpose and means of processing the personal data.
- > **Processing** means any operation, which is performed on personal data or sets of data.
- > **Processor** is an entity which processes personal data on behalf of the controller.

## ✓ Action Points

Test all data sources and processes to ensure that all personal identifiable data collected is used for the specified explicit legitimate purposes as outlined to the data subject.

Ascertain if you obtained the data with the explicit consent or by performance of a contract?

Identify what processing is being done on the data.

Is it being processed manually or automatic and see how secure it is.

Continuously review if the data obtained is being processed in a fair and lawful manner.

Review all areas in your business where data is stored so as to limit the data use to defined purposes.

Ascertain if any of the data is personally identifiable and that you still need it or not.

Ensure all links to data, backups and audit logs, recordings, paper archives containing personally identifiable data are known. You will need to know this for your retention policy to ensure it is not kept for longer than needed.

## PART 4

# Perform an assessment of your system



## Under GDPR Article 35:

If processing data especially if using newer technologies is likely to result in a high risk to the rights of a data subject, then carry out an assessment prior to processing the data. **The Controller shall seek the advice from the Data Protection Officer.**

A Data Protection Impact Assessment is a systematic review of any and all files physical or digital, folders, applications, servers both physical or cloud based, user interfaces, or external storage to assess first what Personally Identifiable data is on them.

Next the processes moves into what could happen to the data and what affect would that have on a Data Subject if the data was released in error, printed in error, edited in error, accessed internally, or access externally (hacked), deleted.

**Then measures can be taken to ensure that the data is never put at risk. As below:**

### > Can the data be minimised?

Example of minimisation would be if the name could be replaced with only the first 3 characters of a name. Same for phones numbers and email as it is with credit cards in most systems. So any breach would not be able to identify a customer.

### > Can the data be encrypted?

Does the data need to be seen at all? Can the date be replaced with ##### or \*\*\*\*\*? If a customer's information was released in error but the personally identifiable data was fully encrypted then there is no Data breach.

### > Can the data be pseudonymised?

Pseudonymised Data is created by taking identifying fields within a database and replacing them with artificial identifiers, or pseudonyms. Hence no intrusion will take place on a customer's personally identifiable data.

## ✓ Action Points

Set up a steering group with representative from each department.

Ask them to review each task they perform and list where personally identifiable data is visible.

Then review the output and put in appropriate security measures to protect the data.

## PART 5

# Review and update all your Policies for GDPR compliance



- > All policies must be capable of implementation and enforceable;
- > They must be concise and easy to understand.
- > And above all else they must balance protection with productivity.

## Some key policies that you must have, but also be able to demonstrate adherence to:

### > Privacy Policy

A privacy policy is a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer data.

### > Retention Policy

A Data retention policy defines the policies for data and records management for meeting legal and business data archival requirements.

### > Subject Access Request Policy

A Subject Access Request Policy defines the process for releasing data back to the confirmed Data Subject from the Data Controller. The Data Subject can ask for all to be released or specific data free for the first time. The Data subject can asked what information is stored, how it is being used and processed, who can see it, who is it shared with.

### Some other important policies:

- Data protection impact assessment procedure
- Retention of records procedure
- Privacy procedure
- Training policy
- Information security policy
- International data transfer procedure
- Data portability procedure
- Data protection officer (DPO) job description
- Complaints procedure
- Audit checklist for compliance
- Privacy notice
- Third Party Data Processor Agreements
- Updated Employee Handbook

## ✓ Action Point

Start updating you policies **today**

PART 6

# GDPR Practical Reminders for your Business



<b>DATA</b>	>	We only get the data we NEED to give the service, not what we think we want.
<b>CONSENT</b>	>	We only get the data we NEED to give the service, not what we think we want.
<b>PURPOSE</b>	>	We only use what we tell the customers we use the data for and no more.
<b>RETENTION</b>	>	We only keep the data for as long as lawfully allowed.
<b>OUTSIDE EU</b>	>	We do not transfer the data outside the EU without consent.
<b>DATA PORTABILITY</b>	>	We do not transfer the data outside the EU without consent.
<b>RIGHT TO BE FORGOTTEN</b>	>	We must forget a person's data when asked to do so, unless there is a lawful purpose governed by regulation.
<b>RIGHT TO ACCESS TO DATA</b>	>	We must give data back to a person when requested free of charge on the first request and within a month unless overburdened with requests.
<b>DATA BREACH</b>	>	We must make the Data Breach notification within 72 hours.

PART 7

# Key Questions



Do you know what data you store about a data subject?  
(Live system / Sandbox / Archive)

Do you know if any personally identifiable data is stored  
in the EU or outside the EU?

Do you have a Data Protection Policy?

Do you know if you are a Data Controller?

Do you know if you are a Data Processor?

Do you know what is considered a Data Breach?

Do you know the fines that could be imposed?

Do you know if your Vendor's use sub processors?

Do you have a Breach notification policy?

Do you have cover for the DPO holidays?

Do you what is PII Data?

Phone / Mobile / Email / IP Address  
any data that can identify an  
individual

Do you know how long to store invoices or calls for?

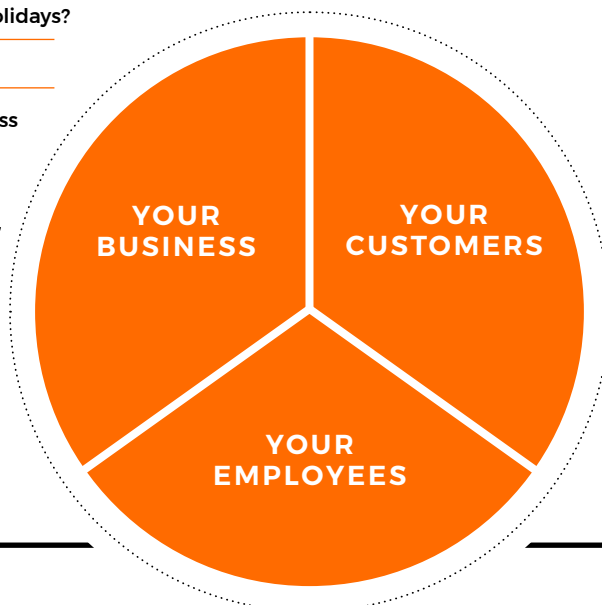
Do you know if you are emailing customers or leads  
who have left your business?

Do you have a Subject Access Request Policy?

Do you know what verification you will require  
for a SAR? Drivers Licence / Passport

Will you save the requests received  
for "Right to be forgotten" ?

Does your Credit Card Merchant provider save  
a customers expired cards?



Do you know how long to store Employee details for?

Have you trained your staff on GDPR?

Do you share data within company groups?

Is company communications limited to EU Only?