GDPR MASTERCLASS

Your GDPR Compliance Checklist

Done	Things to do
	Conduct a data audit of existing customer and supplier data
	List current processes for handling personal data
	Identify your lawful bases for processing, storing, and documenting personal data
	Create a documented process for how you request and record consent
	Write a data protection policy that includes new 'personal data' identifiers (IP addresses, cookies, digital mobile devices)
	Name a specific Data Protection Officer(s) responsible for upholding the policy
	Communicate your new personal data protection policy to all members of the business and make it available for customers to view upon request
	Implement technical processes, such as encryption or levelled access, for existing data
	Create protocols for handling sensitive personal data (genetic and biometric) where relevant
	Create a training procedure for current and new staff responsible for handling data
	Develop a breach notification process (identify, report, manage, resolve, and communicate breaches)
	Write a protocol for data rectification, personal access, data quality, and erasure where it's allowable
	Include clear consent requests on all communications including your website and offline marketing

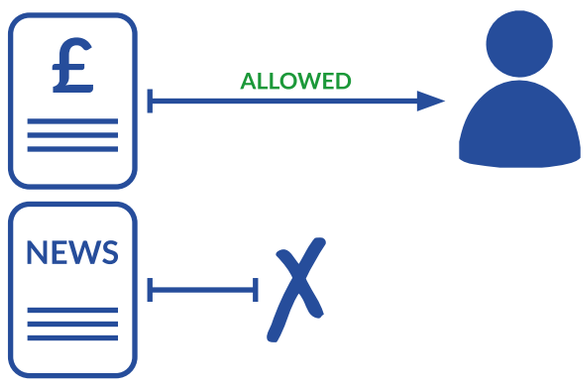
HANDY HINTS

What Do I Need Consent For?

You must obtain consent from customers to contact them for non-transactional communications. For example, if you send your invoices by email, you don't need consent. However, you can't send the same person your email newsletter without them giving explicit consent.

You don't need consent for personal data in the public domain, such as email addresses which are listed on a business website.

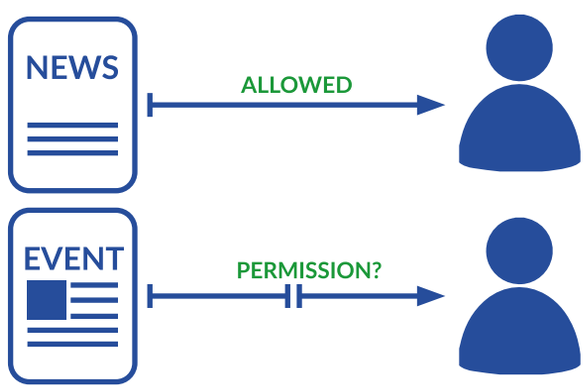
Consent must be freely given and unambiguous. You can't, for example, say that consent is provided for someone to receive marketing telephone calls from you if they have purchased a product from your business. They must explicitly agree to this.



What Is A 'Lawful Basis' For Handling Data?

A lawful basis is when a customer has given you consent to access and use their personal information, or when there is a benefit as a 'legitimate interest' to your business that does not override the fundamental rights of the individual.

For example, a customer must give you permission to allow you to email them a regular newsletter. However, if you are running a local event and want to send direct mail to businesses in the neighbourhood, this is allowable.

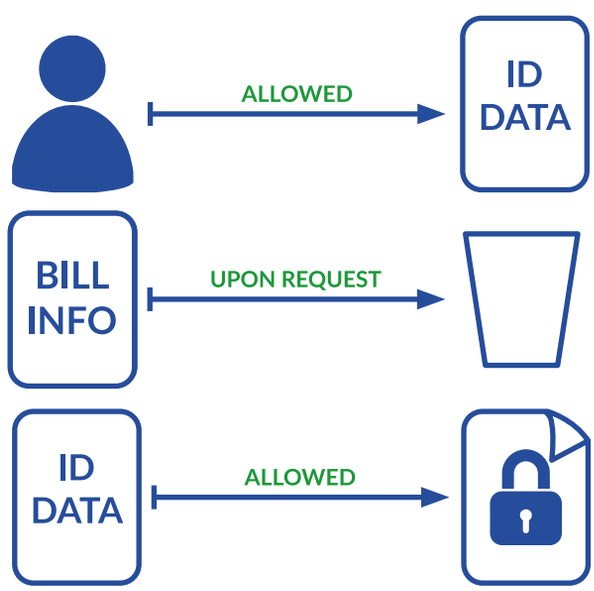


What Is The Right To Erasure?

An individual has the right to request access to view the data you hold on them. You must supply this on request.

They can also ask to be removed entirely from your system, which you must also comply with – although there are a couple of exceptions.

For example, you may remove all data for someone if they have not completed a transaction with your business. You may not, however, remove any financial transactions. To avoid breaching compliance, it is recommended that records with a request for erasure that include financial transactions are archived on a separate database that can only be accessed by limited individuals.



*This email master class/ blog series has been prepared by instantprint as a condensed summary of GDPR and not as a full comprehensive review. We advise all readers to undertake their own further reading and research into GDPR, including a review of the GDPR guidance set out on the Information Commissioner's Office's website.