CHECKLIST | OBTAINING CONSENT UNDER THE GDPR

Presented by GS Group

On 25 May 2018, the General Data Protection Regulation (GDPR) comes into effect in the EU and across the United Kingdom. The GDPR replaces the Data Protection Act and ushers in expanded rights to individuals and their data, and places greater obligations on businesses and other entities that process personal data.

While the GDPR includes a number of important changes regarding cyber-security and data management, one of the most important changes involves strengthening the standards of obtaining consent to process data. Failure to obtain proper consent to process data, which includes contacting individuals, risks whopping fines. The GDPR's maximum fine tops out at €20 million, or 4 per cent of global turnover, whichever is higher. The consequences are steep and there is no room for error.

But GS Group is here with guidance from the Information Commissioner's Office (ICO) to help your business obtain consent from prospects and clients while staying compliant with the GDPR. Use the following checklist and best practice guidance to examine your own consent processes.

To comply with the GDPR's consent requirements and decide whether your existing consents meet the new, higher GDPR standard, your consent mechanisms should demonstrate the following:

- **Unbundled:** Consent requests must be separate from other terms and conditions.
- **Active opt-in:** Pre-ticked opt-in boxes are invalid—instead use unticked opt-in boxes or similar active opt-in methods, such as a binary choice given equal prominence.
- **Granular:** Give granular options to consent separately to different types of data processing wherever appropriate.
- **Named:** Name your organisation and any third parties who will be relying on the consent.
- **Documented:** Keep records to demonstrate what individuals have consented to, including what they were told, and when and how they consented.
- **Easy to withdraw:** Tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to consent, meaning you need to have simple and effective withdrawal mechanisms in place.
- **No imbalance in the relationship:** Consent will not be 'freely given' if there is an imbalance in the relationship between the individual and data controller.

ASKING FOR CONSENT	YES	NO	ADDITIONAL NOTES
We have checked that consent is the most appropriate lawful basis for processing.	☐	☐	
We have made the request for consent prominent and separate from our terms and conditions.	☐	☐	
We ask people to positively opt in.	☐	☐	
We do not use pre-ticked boxes or any other type of consent by default.	☐	☐	
We use clear, plain language that is easy to understand.	☐	☐	

ASKING FOR CONSENT, continued	YES	NO	ADDITIONAL NOTES
We specify why we want the data and what we are going to do with it.	☐	☐	
We give granular options to consent to independent processing operations.	☐	☐	
We have named our organisation and any third parties.	☐	☐	
We tell individuals they can withdraw their consent.	☐	☐	
We ensure that the individual can refuse to consent without harm.	☐	☐	
We do not make consent a precondition of service.	☐	☐	
If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.	☐	☐	

Can I use existing Data Protection Act consents?

Remember that, although you are not required to automatically 'repaper' or refresh all existing Data Protection Act (DPA) consents in preparation for the GDPR, it is important to check your processes and records in detail to be sure existing consents meet the GDPR standard.

If your existing DPA consents ***do not*** meet the GDPR's high standards or are poorly documented, you will need to seek new GDPR-compliant consent.

How should I write a consent request?

Consent requests need to be prominent, concise, easy to understand and separate from any other information, such as general terms and conditions. Use the following best practices as guidance:

- Keep your consent requests separate from other general terms and conditions, and clearly direct people's attention to them.
- Use clear, straight-forward language.
- Adopt a simple style that your intended audience will find easy to understand.
- Avoid technical jargon and confusing terminology, such as double negatives.
- Use consistent language and methods across multiple consent options.
- Keep your consent requests concise and specific, and avoid vague or blanket wording.

What information should I include in my consent requests?

Consent requests should, at a minimum, include the following:

- The name of your organisation and the names of any third parties who will rely on the consent
- Why you want the data
- What you will do with the data
- That people can withdraw their consent at any time

.

What methods can I use to obtain consent?

Whatever method you use must meet the standard of an unambiguous indication by clear, affirmative action. This means you must ask people to actively opt in. Examples of active opt-in mechanisms include the following:

- Signing a consent statement or paper form
- Ticking an opt-in box on paper or electronically
- Clicking an opt-in button or link online
- Selecting from equally prominent yes or no options
- Choosing technical settings or preference dashboard settings
- Responding to an email requesting consent
- Answering yes to a clear oral consent request

RECORDING CONSENT	YES	NO	ADDITIONAL NOTES
We keep a record of when and how we got consent from the individual.	☐	☐	
We keep a record of exactly what the individual was told at the time.	☐	☐	

How should I record consent?

You must have an effective audit trail of how and when consent was given, so you can provide evidence if challenged. Good records will also help you monitor and refresh consent as appropriate. You must keep good records that demonstrate the following:

- **Who consented:** The name of the individual or other identifier
- **When they consented:** A copy of a dated document or online record that includes a timestamp; or, for oral consent, a note of the time and date that was made at the time of the conversation
- **What they were told at the time:** A master copy of the document or data capture form containing the consent statement in use at that time, along with any separate privacy policy, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time.
- **How they consented:** For written consent, a copy of the relevant document or data capture form. If consent was given online, your records should include the data submitted as well as a timestamp to link it to the relevant data capture form. If consent was given orally, you should keep a note of this made at the time of the conversation—it does not need to be a full record of the conversation.
- **Whether they have withdrawn consent:** And, if they have, when they withdrew their consent.

MANAGING CONSENT	YES	NO	ADDITIONAL NOTES
We regularly review consent to check that the relationship, the processing and the purposes have not changed.	☐	☐	
We have processes in place to refresh consent at appropriate intervals, including any parental controls.	☐	☐	
We consider using privacy dashboards or other preference management tools as a matter of good practice.	☐	☐	

.

MANAGING CONSENT, continued	YES	NO	ADDITIONAL NOTES
We make it easy for individuals to withdraw their consent at any time and publicise how to do so.	☐	☐	
We act on withdrawals of consent as soon as we can.	☐	☐	
We do not penalise individuals who wish to withdraw consent.	☐	☐	

How should I manage consent?

Your obligations do not end when you get consent. You should view consent as a dynamic part of your ongoing relationship of trust with individuals, not a one-off compliance box to tick and file away. To reap the benefits of consent, you need to offer ongoing choice and control. It is good practice to provide preference management tools like privacy dashboards to allow people to easily access and update their consent settings. Find more ICO guidance on these tools by clicking here.

You should keep your consents under review. You will need to refresh them if anything changes—for example, if your processing operations or purposes evolve, the original consent may not be specific or informed enough. If you are in doubt about whether the consent is still valid, you should refresh it.

You should also consider whether to automatically refresh consent at appropriate intervals. How often it is appropriate to do so will depend on the particular context, including people's expectations, whether you are in regular contact and how disruptive repeated consent requests would be to the individual. If in doubt, the ICO recommends you consider refreshing consent every two years. If you are not in regular contact with individuals, consider sending occasional reminders of their right to withdraw consent and how to do so.

How should I manage the right to withdraw consent?

The GDPR gives people a specific right to withdraw their consent. You will need to ensure that you put proper withdrawal procedures in place. As the right to withdrawal is at any time, it is not enough to provide an opt-out only by reply. Individuals must be able to opt out at any time they choose, on their own initiative. It must also be as easy to withdraw consent as it was to give it. This means the process of withdrawing consent should be an easily accessible one-step process. If possible, individuals should be able to withdraw their consent using the same method as when they gave it.

It is good practice to publicise both online preference management tools and other ways of opting out, such as customer service phone numbers. You should bear in mind that not everyone is comfortable with technology or has access to the internet. If someone originally gave consent on paper or in person, it may not be enough to offer only an online opt-out.

It is also good practice to provide both anytime opt-out mechanisms, such as privacy dashboards, and opt-out by reply to every contact. This could include an unsubscribe link in an email or an opt-out phone number, address or web link printed in a letter.

If someone withdraws consent, you should stop the processing immediately, particularly in an online automated environment. However, in other cases, you may be able to justify a short delay while you process the withdrawal. You must include details of the right to withdraw consent in your privacy notices and consent requests. It is best practice to also include details of how to withdraw consent.

For more information on cyber best practices, contact the insurance professionals at GS Group by calling 01738 441 555 or visiting www.gs-group.uk.com today.

.