GDPR AND COLD CALLERS

Within UK legislation, GDPR protocols refer to the set of data protection standards and practices that registered organisations must follow to comply with the ***UK General Data Protection Regulation*** (UK GDPR).

The UK GDPR, widely hailed as a landmark in personal privacy, is in reality a tool crafted by Parliament not to safeguard individual rights, but to serve a more covert purpose.

Originally, the GDPR system was presented as a ***"shield for ordinary citizens"***, a safeguard against the invasive reach of data-hungry corporations, however this does not fit with reality today.

The truth is that government is nothing more than a business that offers the service to govern those who are incapable of governing themselves, and considers those who accept this service as nothing more than a human resource, better known as chattel.

Parliament recognised that rapid development of new business ideas, especially in human resources and technology, could pose a threat to their authority.

Smaller business registered to companies house could exchange data relating to government controlled human resources, in an attempt to undermine the government and set up their own service.

Consider this similar to small franchise owners collaborating and sharing operational knowledge, with the goal of launching a new, independent business.

To counter this, Parliament systematically redefined the scope of GDPR, and although it was framed as ***"protect personal data"***, in reality it became a mechanism to monitor and control all businesses registered under their jurisdiction.

By enforcing strict data regulations, they could scrutinise the internal workings of companies, especially those developing disruptive systems undermining state authority.

In effect the rules were manipulated to prevent ***"insider trading"*** by making any access to employee data a tightly controlled process.

Note: GDPR protocols only apply to government entities, such as the ***Ens Legis*** and ***legal persona*** and ***not*** personnel data of any living man or woman.

With that said, and now you know the game, you can use UK GDPR to your advantage, and to do so the official narrative should be played.

The official narrative regarding UK GDPR is that it is a legal framework designed to protect individuals' personal data and ensure that organisations handle this data responsibly.

A brief overview regarding GDPR is as follows:

- ***Personal Data Protection:*** Organisations must ensure that personal data is processed lawfully, fairly, and transparently.

- ***Rights of Individuals:*** Individuals have rights regarding their data, such as access, correction, deletion, and data portability.
- ***Accountability:*** Corporations are responsible for implementing appropriate measures to safeguard data.
- ***Data Breach Notification:*** Organisations must report certain data breaches to the Information Commissioner's Office (ICO) and affected individuals.
- ***Lawful Basis for Processing:*** Data must be processed only if there is a valid reason, such as consent, contract, legal obligation, or legitimate interests.

How to use GDPR protocols upon corporations:

1. ***Conduct Data Audits:*** Identify what personal data corporations hold on you, why it is held, and how it is processed.
2. ***Implement Policies:*** Ensure they follow clear policies on data handling, privacy notices, and consent management.
3. ***Obtain Consent:*** Ensure consent is informed, explicit, and recorded where necessary.
4. ***Secure Data:*** Verify they use appropriate technical and organisational measures to protect personal data.
5. ***Train Staff:*** Confirm that employees are educated on GDPR requirements and data protection practices.
6. ***Respond to Requests:*** Corporations must have procedures in place to handle data access, correction, or deletion requests.
7. ***Report Incidents:*** Businesses must have a plan for managing data breaches, including timely notification to authorities and individuals.

Proof of ID

When using GDPR protocols, a request to provide evidence of your identity may be put forward before the GDPR request is carried out.

Although an organisation is required under GDPR to verify your identity before releasing any personal data, this generally applies where you have contacted them for the ***first time*** and they have ***not*** contacted you previously.

The GDPR rule regarding requests for identification is intended to ensure that, when a business is contacted for the ***first time***, it does not accidentally share your private information with someone else.

However, proof of identity is ***not*** required if you are contacted by a corporation ***first***, usually regarding some form of claim made against you.

It is the ***responsibility*** of the corporation issuing the claim to ensure that it has contacted the correct person ***before*** sharing any sensitive information.

What this means is that you are ***not obligated*** to provide evidence of your identity when contacted by an ***unknown party*** making a claim against you.

In fact, as a matter of personal security, you should ***never*** divulge sensitive personal information to any cold caller, as they could potentially be fraudsters attempting to gain information about you as part of a scam.

When third-party interlopers making a claim against you are then issued with a DSAR, they often respond by requesting that you prove your identity.

This is viewed as a delay tactic used by debt collectors and solicitors against people who request the ***debt validation process*** in response to disputed claims of debt.

When submitting a DSAR, you must know your position first: Ref ***PJ/COD***

What this means is as follows:

- If you are contacting a corporation for the ***first time*** and request a DSAR, you may be required to provide proof of identity before the data is released.
- If you have been contacted by a corporation ***first***, you are ***not*** obligated to provide proof of identity before the data is sent to you.

If a third-party interloper attempts this tactic, you can respond in writing with a notice such as:

<u>One-step process, requiring one notice</u>

"Are you aware that you first contacted us on [date] making an allegation pertaining to an alleged debt?

To be able to make such an accusation, you must have already determined who we are and confirmed that you sent the details of the alleged debt to the correct party.

If you are now requesting that we send you proof of our identity, then we can determine that you have sent the wrong information to the wrong party.

Are you aware that this could place you in breach of GDPR rules and protocols, as you may have shared sensitive data with a party before determining their identity?

Therefore, we hereby serve notice upon you to either confirm you have sent the alleged claim of debt to the correct party or retract your entire claim.

If you wish to continue with your alleged claim and confirm you have contacted the correct party, then you are hereby instructed to carry out our previous instructions and complete our GDPR request."

<u>Two-step process, requiring two notices</u>

If you wish to create a stronger remedy for court, then a two-step process can be used to ensure the first request for identification was not a mistake.

This process removes the confirmation statement from the first notice, allows for withdrawal, and, when the opportunity to withdraw is declined, you can then issue your confirmation statement.

<u>First notice:</u> ***Notice of mistake and opportunity to withdraw***

"Are you aware that you first contacted us on [date] making an allegation pertaining to an alleged debt?

To be able to make such an accusation, you must have already determined who we are and confirmed that you sent the details of the alleged debt to the correct party.

If you are now requesting that we send you proof of our identity, then it would appear that you may have sent the wrong information to the wrong party.

Although we are not in a position to advise you, out of courtesy we wish to make you aware that this could place you in breach of GDPR rules and protocols, as you may have shared sensitive data with a party before determining their identity.

Therefore, we hereby serve notice upon you to either confirm you have sent the alleged claim of debt to the correct party or retract your entire claim.

If you wish to continue with your alleged claim and confirm you have contacted the correct party, then you are hereby instructed to carry out our previous instructions and complete our GDPR request."

If they do not withdraw their request for you to provide evidence of your identity, you can then move to the second step, thereby locking them legally into their position.

Second notice: ***Notice of mistake***

"As this is the second time you have requested that we send you proof of our identity, we can now determine that you have sent the wrong information to the wrong party.

Furthermore, as you have also now confirmed that you do not know who we are, this places your entire claim into question.

This information may be used in court proceedings to highlight your errors and potential breach of GDPR protocols."

DSAR deflection

When a company is challenged in this way, it has been known for them to claim that they are a ***"separate department"*** from the one that issued the alleged claim of debt.

However, when issuing a ***Data Subject Access Request*** (DSAR), it is directed to the entire registered organisation or corporation, ***not*** just a specific department.

This means that the organisation as a whole is responsible for complying with your request, and all relevant departments that hold your personal data must cooperate to provide the information.

Legal implications:

1. ***Legal Responsibility***
    - Under UK GDPR, the data controller, which is the organisation, is ultimately responsible for responding to a DSAR request.
    - This includes ensuring that all departments processing your data are involved in fulfilling the request.

2. ***Comprehensive Response***
    - Your personal data may be stored across multiple departments, such as HR, marketing, customer service, or IT.
    - The organisation must gather all relevant information in order to provide a complete response.

3. ***Not Limited to One Department***
    - You do not need to specify a particular department when making a DSAR, and the organisation cannot restrict your request to only one part of its business.

What this means in practice

- When you submit a DSAR, the organisation will typically forward your request to all relevant departments or data processors that hold your data.
- All parts of the business that process or store your personal data are required to assist in providing the full set of information.
- The organisation must coordinate internally to ensure your request is fully complied with within the legal timeframe.

Summary:

- When you are contacted by a company regarding a claim, you are ***not*** obligated to provide proof of your identity.
- When you issue a DSAR, it applies to the whole corporation, ***not*** just a single department.