GIBRALTAR REGULATORY AUTHORITY

(13) Guidance on Consent

Guidance on the EU General Data Protection Regulation 2016/679 and the Data Protection Act 2004

DISCLAIMER

Please note that, on 1st January 2021, the EU General Data Protection Regulation 2016/679 ("EU GDPR") was superseded by the Gibraltar General Data Protection Regulation. The legislation however remains largely the same, and therefore, the general principles relating to the EU GDPR as may be referenced within this Guidance Note, continue to apply to the current regime.

21st December 2020

Guidance Note IR01/19 (v2)

FOREWORD

The EU General Data Protection Regulation 2016/679 (the "GDPR") came into force on 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive 95/46/EC.

Her Majesty's Government of Gibraltar amended the Data Protection Act 2004 (the "DPA") on 25th May 2018, in accordance with the introduction of the GDPR. The DPA complements the GDPR and also implements the Law Enforcement Directive 2016/680. Therefore, the DPA and the GDPR must be read side by side.

It is important to note that the GDPR does not generally require transposition (EU regulations have 'direct effect') and automatically became law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR and/or the DPA will impose on them. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority, as the Information Commissioner, is aware of the increased obligations that the GDPR and DPA place on organisations. The Information Commissioner's aim is to alleviate some of the concerns for businesses, public-sector and third-sector organisations and assist them ensure data protection compliance.

SUMMARY

- Consent is one of the lawful grounds for the processing of personal data under Article 6 of the GDPR. Explicit consent is one of the lawful bases that can be relied on to process special categories of personal data or personal data relating to criminal convictions and offences.

- For consent to be valid, it must meet the following conditions –

  1) Freely given. Consent must be freely given, which requires the following:

     a. *Imbalance of power.* Where there is an imbalance of power, consent is unlikely to be valid.

        i. It is unlikely that public authorities can rely on consent for the processing of personal data as there is often a clear imbalance of power in the relationship between the data controller and the data subject.
        ii. An imbalance of power also occurs in the employment context. In the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to the processing of their personal data without detrimental effects as a result of a refusal.

     However, it's important to note that in certain circumstances, employers and public authorities may rely on consent as a lawful basis for processing, as long as they can demonstrate that consent is freely given (for example, a film crew wants to film a certain part of an office).

     b. *Conditionality.* The purpose of the processing of personal data should not be disguised nor bundled with the provision of a contract of a service for which personal data are not necessary.

     c. *Granularity*. Where a service involves multiple processing operations for more than one purpose, data subjects should be free to choose which purpose they accept instead of having to consent to a bundle of processing purposes.

     d. *Detriment.* Data controllers should demonstrate that it is possible for a data subject to refuse or withdraw consent without detriment.

  2) Specific. Consent must be given in relation to a specific purpose. This requirement should be interpreted in line with the requirement for 'granularity' to obtain free consent.

  3) Informed. Providing information to data subjects prior to obtaining their consent is essential to allow them to make informed decisions, understand what they are agreeing to and be able to exercise their right to withdraw consent. If the target audience includes individuals that are underage, data controllers are expected to make sure that the information provided is understandable for minors.

  4) Unambiguous. Consent requires an unambiguous indication by means of a statement or by a clear affirmative action from the data subject.

- Explicit consent plays a role in the processing of special categories of personal data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards and on automated individual decision-making, including profiling.

- Data controllers must be able to demonstrate a data subject's consent. This means that the burden of proof will be on the data controller.

- Data controllers must ensure that consent can be withdrawn by the data subject and that consent must be as easy to withdraw as it was to give.

CONTENTS

1. INTRODUCTION

This guidance note provides information and guidance on the conditions for consent under the Data Protection Act 2004 ("DPA") and the EU General Data Protection Regulation 2016/679 ("GDPR"). It's important to note that the concept of consent is not new, as its definition and role remains similar to that under the previous EU Data Protection Directive 95/46/EC and the current ePrivacy Directive 2002/58/EC (the "ePrivacy Directive").

Consent is one of the six lawful bases to process personal data under Article 6 of the GDPR. When initiating activities that involve processing of personal data, data controllers should take time to consider what would be the appropriate lawful ground for the envisaged processing.

Generally, consent can only be an appropriate lawful basis if individuals are offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. As a result, before asking for consent, data controllers should assess whether they will meet the requirements to obtain valid consent under the GDPR.

Obtaining consent does not negate or in any way diminish a data controller's obligation to comply with the principles of data processing of the GDPR, especially those relating to fairness, necessity and proportionality. Even if the processing of personal data is based on consent, this would not legitimise the collection of personal data which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.

The Information Commissioner[1] is aware of the review of the ePrivacy Directive, implemented in Gibraltar under the Communications (Personal Data and Privacy) Regulations 2006. However, the notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR[2].

Data controllers are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including those by the use of cookies, apps or other software. In this respect, the European Data Protection Board ("EDPB") have provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy[3].

Note: *this document largely aims to provide guidance in line with the EDPB's guidelines on consent under the GDPR[4]. For more detailed guidance it may be useful for data controllers to consult said guidelines separately.*

[1] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

[2] Under Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Article 4(11) and Article 7 of the GDPR apply.

[3] See European Data Protection Board statement on ePrivacy dated 25/05/2018 and European Data Protection Board Statement 3/2019 on an ePrivacy regulation.

[4] See European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (Version 1.1) (4th May 2020). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

2. CONSENT UNDER THE GDPR AND DPA

GDPR - Article 4(11)

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Consent is one of the lawful grounds for the processing of personal data under Article 6 of the GDPR. The GDPR provides additional guidance in Article 7 and in Recitals 32, 33, 42 and 43 in respect of how data controllers must act to comply with the consent requirements.

The GDPR includes specific provisions and recitals on the withdrawal of consent. This means that consent should be a reversible decision and that data subjects should have a degree of control in respect of the processing of their personal data.

Elements of valid consent

In the following, the wording of Article 4(11) of the GDPR is analysed, and guidance is provided for data controllers to ensure compliance with the GDPR[5].

Freely given

Data subjects should have a real choice and control over the processing of their personal data. The GDPR prescribes that if a data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid[6].

For example, consent will not be considered freely given if it's bundled as a non-negotiable part of terms and conditions or if data subjects are unable to refuse or withdraw consent without detriment (see Recitals 42 and 43 of the GDPR).

When assessing whether consent is freely given, data controllers should consider, amongst other things, the specific situation of tying consent into contracts or the provision of a service (see Article 7(4) of the GDPR). In general terms, any element of inappropriate pressure or influence upon the data subject which prevents him/her from exercising their free will, shall render consent invalid.

i. Imbalance of power

Recital 43 of the GDPR indicates that it is unlikely that public authorities can rely on consent for the processing of personal data as there is often a clear imbalance of power in the

[5] For guidance with regard to ongoing processing activities based on consent under the previous EU Data Protection Directive 95/46/EC, refer to Recital 171 of the GDPR.

[6] See European Data Protection Board, Opinion 15/2011 on the definition of consent (WP187), Page 12 (13 July 2011).

relationship between the data controller and the data subject. Therefore, the Information Commissioner is of the view that public authorities should consider other lawful bases for the processing of personal data[7].

Notwithstanding the above, the use of consent as a lawful basis for data processing by public authorities is not totally excluded. In some cases, public authorities may rely on consent as the lawful basis for data processing. For example, a public school asks students for consent to use their photographs in a printed school magazine. In this case, students have a genuine choice as they will not be denied education or services and can refuse the use of their photographs without any detriment.

An imbalance of power also occurs in the employment context[8]. In the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to the processing of their personal data without detrimental effects as a result of a refusal. Further, it is unlikely that the data subject is able to respond freely to a request for consent from his/her employer (for example, where consent is sought for monitoring systems such as camera observation in a workplace). Employers should therefore not rely on consent of the employees as the lawful basis for the processing of their personal data[9].

However, it's important to note that in certain circumstances, employers may rely on consent as a lawful basis for processing, as long as they can demonstrate that consent is freely given (for example, a film crew wants to film a certain part of an office. In this case, the employer may ask its employees, who work in that part of the office, for their consent to be filmed. Those who don't want to be filmed are not penalised in any way but instead are provided with desks elsewhere in the building where they may continue to work during the duration of the filming).

ii. Conditionality

Article 7(4) of the GDPR plays an important role when it comes to assessing whether consent is freely given. It seeks to ensure that the processing of personal data for which consent is sought is not directly or indirectly the counter-performance of a contract. If a request for consent is tied to the performance of a contract by the data controller, then a data subject who does not consent to making their personal data available for processing by the data controller, runs the risk of being denied services they have requested. In other words, if the data subject wishes to enter into a contract, but the condition for entering into said contract is that the individual must consent to the processing of personal data which is **not necessary for the performance of the contract**, then consent is not considered to have been freely given and the requirements of the GDPR regarding consent would not have been met. If, however, the same data controller also offers the exact service and contract but without the need for consent to personal data processing, then individuals choosing the option requiring personal data to be provided, would be considered as having freely given consent.

---

[7] Please see the Information Commissioner's Guidance Note, "(6) Identifying the 'Lawful Basis'" available here: https://www.gra.gi/data-protection/guidance

[8] See Article 88 of the GDPR, which refers to the processing in the context of employment and Recital 155 of the GDPR.

[9] See European Data Protection Board, Opinion 2/2017 on data processing at work (WP249), Pages 6-7 (8 June 2017).

Data controllers should determine what the scope of the contract is and what personal data is **necessary** for the performance of that contract[10]. There needs to be a direct and objective link between the processing of personal data and the purpose of the execution of the contract. If a data controller seeks personal data that is **necessary for the performance of a contract**, then, although consent under Article 6(1)(a) of the GDPR would not be the appropriate lawful basis, they would still have a lawful basis under Article 6(1)(b) of the GDPR[11].

In regard to the provision of online services, access to said services should not be made conditional on the consent of a user to the storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a user. For example, where a user wishes to contract a service through a website, but access to the content of the website is dependent on the individual consenting to the use of cookies by the data controller, consent will not be considered freely given as the user is not presented with a genuine choice.

iii. Granularity

In general terms, where a service involves multiple processing operations for more than one purpose, data subjects should be free to choose which purpose they accept instead of having to consent to a bundle of processing purposes (see Recital 43 of the GDPR). In these cases, several consents may be warranted in order to offer a service, pursuant to the GDPR (see Recital 32 of the GDPR).

The above means that if a data controller has combined several purposes for processing and has not attempted to seek separate consent for each purpose, consent will not be considered freely given and therefore, not valid. This granularity is closely related to the need for consent to be specific (see below).

iv. Detriment

Data controllers should demonstrate that it is possible for a data subject to refuse or withdraw consent without detriment (see Recital 42 of the GDPR). Examples of detriment include deception, intimidation, coercion, negative consequences, a clear disadvantage or costs incurred by the data subject if he/she refuses or withdraws consent.

If a data controller demonstrates that a service includes the possibility to withdraw consent without any detriment to the user, this may serve to show that consent was freely given. In this respect, the GDPR does not preclude all incentives but places the onus on the data controller to demonstrate that consent was freely given in all the circumstances.

[10] See European Data Protection Board, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), Pages 16-17 (9 April 2014).

[11] Article 6(1)(b) of the GDPR provides a lawful basis where *"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".*

Specific

Article 6(1)(a) of the GDPR states that consent must be given in relation to one or more specific purposes. This means that data subjects should have a choice in relation to each purpose[12].

The requirement for consent to be specific is to ensure a level of user control and transparency for the data subject. This requirement should be interpreted in line with the requirement for 'granularity' to obtain free consent (see Recital 43 of the GDPR).

To comply with the element of 'specific', data controllers must apply the following:

- purpose specification;
- granularity in consent requests; and
- clear separation of information relating to the obtaining of consent from information relating to other matters.

Informed

The requirement for transparency is one of the fundamental principles of the GDPR and is closely related to the principles of fairness and lawfulness (see Article 5 of the GDPR). Therefore, providing information to data subjects prior to obtaining their consent is essential to allow them to make informed decisions, understand what they are agreeing to and be able to exercise their right to withdraw consent.

If a data controller does not comply with the requirements for informed consent, then consent will be deemed invalid and the data controller may be in breach of Article 6 of the GDPR.

For consent to be informed, data controllers should provide individuals with the necessary information to allow them to make an informed choice. Therefore, the Information Commissioner recommends that at least the following information is provided –

- the data controller's identity;
- the purpose of each of the processing operations for which consent is sought;
- the type of data that will be collected and used;
- the right to withdraw consent (see Article 7(3) of the GDPR);
- information regarding the use of data for automated decision-making (see Article 22(2)(c) of the GDPR) where relevant; and
- the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards (see Article 46 of the GDPR).

Data processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, data controllers must provide a full list of recipients or categories of recipients including data processors.

In respect of how information is provided to individuals, the GDPR does not prescribe the form or shape in which information must be provided to fulfil the requirement of informed consent. However, the GDPR puts several requirements for informed consent, mainly in Article 7(2) and Recital 32 of the GDPR.

Data controllers should also assess their target audience when providing information. For example, if the target audience includes individuals that are underage, data controllers are

[12] See European Data Protection Board, Opinion 3/2013 on purpose limitation (WP203), (2 April 2013).

expected to make sure that the information provided is understandable for minors (see Recital 58 of the GDPR).

Unambiguous indication of wishes

Article 4(11) of the GDPR makes it clear that consent requires an unambiguous indication by means of a statement or by a clear affirmative action from the data subject. In general terms, it must be obvious that the individual has consented to the particular processing of their data.

A clear affirmative action means that the individual must have taken a deliberate action to consent to the particular processing (see Recital 32 of the GDPR). The use of pre-ticked opt-in boxes is invalid under the GDPR. Further, silence or inactivity from the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.

Data controllers should note that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Data controllers should design consent mechanisms in ways that are clear to data subjects. They should also avoid ambiguity and ensure that the action by which consent is given can be distinguished from any other actions. For example, in an online context, continued use of a website by a user is not conduct from which a data controller can infer consent by the data subject to his/her personal data being processed. This is because actions such as scrolling or swiping through a website can be difficult to distinguish from other activity or interaction by the user, and therefore, determining that an unambiguous consent has been obtained may not be possible.

Data controllers should also consider whether they can avoid the need for multiple consent requests, in particular for the processing of personal data in the digital context. Multiple consent requests that require answers from users through clicks and swipes may cause a degree of click fatigue, which may diminish the warning effect of consent mechanisms at a risk to the data subjects.

Most importantly, data controllers should obtain consent before they start processing personal data for which consent is needed.

3. EXPLICIT CONSENT

Under the GDPR, explicit consent plays a role on the processing of special categories of personal data (see Article 9 of the GDPR), the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards (see Article 49 of the GDPR) and on automated individual decision-making, including profiling (see Article 22 of the GDPR).

The term 'explicit' refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. A way of obtaining explicit consent is to expressly confirm consent in a written statement. Where appropriate, the written

statement should be signed by the data subject to remove all possible doubt and potential lack of evidence in the future[13].

In terms of obtaining explicit consent in the digital or online context, a data subject may provide the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject or by using an electronic signature.

In respect of the use of oral statements, these can be sufficiently express to obtain valid explicit consent. However, the use of oral statements may make it difficult for data controllers to prove that all conditions for valid explicit consent were met when the statement was recorded.

Explicit consent may be obtained through a telephone conversation. However, data controllers should ensure that information about the choice is fair, intelligible and clear, and that it asks for a specific confirmation from the data subject (for example, pressing a button or providing oral confirmation).

Explicit consent may also be obtained from a visitor to a website if a data controller offers an explicit consent screen that contains 'Yes' and 'No' boxes which clearly indicate the need for consent. In this regard, data controllers must still ensure that the conditions for obtaining valid consent under the GDPR are met (for example, informed consent).

Two stage verification of consent is another method that may be used to make sure explicit consent is valid. For example, a data controller sends an email to a data subject requiring their explicit consent for the processing of their personal data. The email explains the need for consent to the use of the data for a specific purpose. If the data subject agrees to said use of their personal data, the controller then asks the data subject to send an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.

4. ADDITIONAL CONDITIONS FOR OBTAINING VALID CONSENT

Article 7 of the GDPR sets out additional conditions for obtaining valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent. The additional conditions under Article 7 of the GDPR apply to consent referred to in other articles of the GDPR.

In the following, guidance is provided in respect of the additional requirement to demonstrate valid consent and on the right to withdraw consent.

Demonstrating consent

[13] See European Data Protection Board, Opinion 15/2011 on the definition of consent (WP187), Page 25 (13 July 2011)

Article 7(1) of the GDPR prescribes that data controllers must be able to demonstrate a data subject's consent. This means that the burden of proof will be on the data controller (see Recital 42 of the GDPR).

Data controllers are free to develop methods to comply with this provision. However, the duty to demonstrate that valid consent has been obtained should not in itself lead to excessive amounts of additional data processing. This means that the data controller should only obtain enough data to show consent was obtained but not collect any more information than necessary.

Data controllers must be able to demonstrate consent for as long as the data processing activity lasts. After the processing activity ends, proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, in accordance with Article 17(3)(b) and 17(3)(e) of the GDPR.

The GDPR does not impose a specific time limit in respect of how long consent will last. How long consent lasts will depend on the context, scope of the original consent and the expectations of the data subject. However, if the processing operations change or evolve considerably, then the original consent will no longer be valid and new consent will need to be sought.

Withdrawing consent

Article 7(3) of the GDPR prescribes that data controllers must ensure that consent can be withdrawn by the data subject and that consent must be as easy to withdraw as it was to give.

The GDPR does not state that giving and withdrawing consent must always be done through the same action. However, when consent is obtained via electronic means through only one mouse-click, swipe or keystroke, data subjects must, in practice, be able to withdraw consent equally as easily. If consent is obtained through the use of a service-specific user interface, the data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the purpose of withdrawing consent would require undue effort.

Data subjects should be able to withdraw consent without detriment. This means that data controllers must, where possible, make withdrawal of consent free of charge or without lowering service levels[14].

Easy withdrawal of consent is a necessary aspect of valid consent under the GDPR. Therefore, if the withdrawal right does not meet GDPR standards, then the consent mechanism used by a data controller would not comply with the GDPR.

[14] See European Data Protection Board, Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP174) and Opinion 5/2005 on the use of location data with a view to providing value-added services (WP115).

5. CONSENT AND OTHER LAWFUL GROUNDS IN ARTICLE 6 OF THE GDPR

Article 6 of the GDPR describes six lawful bases on which a data controller can rely on for the processing of personal data. The application of one of these six lawful bases must be established prior to the data controller undertaking the processing activity and in relation to a specific purpose.

If a data controller decides to rely on consent for the processing of personal data, they must be prepared to stop the processing if the data subject withdraws consent. Relying on consent when the data controller can rely on other lawful bases for the processing of personal data would be fundamentally unfair to the data subjects.

The above means that data controllers cannot swap from consent to other lawful bases for the processing of personal data.

6. AREAS OF CONCERN IN THE GDPR

Children's data

Article 8 of the GDPR and section 11 of the DPA introduce additional obligations to ensure an enhanced level of data protection for children in relation to information society services[15]. The reasons for the enhanced protection are specified in Recital 38 of the GDPR.

In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old[16]. Therefore, if the child is below the age of 13 years, the processing shall be lawful only if consent is given or authorised by the holder of parental responsibility over the child.

Scientific research

The term 'scientific research' is not defined in the GDPR. However, Recital 159 of the GDPR states that the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. Notwithstanding the wording of Recital 159 of the GDPR, the Information Commissioner is of

[15] Article 4(25) of the GDPR states that an information society service means a service as defined in Article 1(1)(b) of Directive 2015/1535 of the European Parliament and of the Council. An indicative list of services not covered by the above definition is set out in Annex I of Directive 2015/1535. See also Recital 18 of Directive 2000/31 of the European Parliament and of the Council.

[16] Article 8 of the GDPR and section 11(a) of the DPA.

the view that the term 'scientific research' should not be stretched beyond its common meaning.

If data controllers rely on consent as the legal basis for conducting research, this consent should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation[17].

It's important to note that consent is not the only legal basis that data controllers may rely on, with regard to the processing of personal data for research purposes. As long as appropriate safeguards are in place, in accordance with Article 89(1) of the GDPR, and the processing is fair, lawful, transparent and complies with the data minimisation principle and individuals' rights, other lawful grounds may be relied on (for example, Article 6(1)(e) or Article 6(1)(f) of the GDPR). The same applies to special categories of personal data pursuant to the derogation of Article 9(2)(j) of the GDPR.

Data subject's rights

Processing activities that rely on consent will affect data subject's rights. For example, data subjects have the right to data portability (see Article 20 of the GDPR) when processing is based on consent. On the other hand, a data subject's right to object (see Article 21 of the GDPR) does not apply when the processing is based on consent, although the right to withdraw consent at any time provides a similar outcome.

Further, the rights provided under Articles 16 to 20 of the GDPR indicate that data subjects have the right to erasure when consent has been withdrawn and the right to restriction, rectification and access[18].

7. CONSENT OBTAINED UNDER THE PREVIOUS EU DATA PROTECTION DIRECTIVE 95/46/EC

Consent obtained prior to the GDPR continues to be valid as long as it meets the conditions for consent in the GDPR. Therefore, data controllers should review their arrangements to ensure they meet the GDPR standard (see Recital 171 of the GDPR).

If data controllers find that the consent obtained prior to the GDPR does not meet the GDPR standard, they will need to take appropriate action to comply with these standards (for example, refreshing consent in a GDPR compliant manner). If a data controller is unable to renew consent to meet the GDPR standard and is also unable (as a one-off situation) to rely

[17] An example of a procedural obligation can be found in the Clinical Trials Regulation (Regulation (EU) No 536/2014 of the European Parliament and of the Council (16th April 2014).

[18] In cases where certain data processing activities are restricted in accordance with Article 18 of the GDPR, consent of the data subject may be needed to lift restrictions.

on a different lawful basis for the processing of personal data, the processing activities must be stopped. In any event, data controllers should observe the principles of lawful, fair and transparent processing.

8. CONSENT IN PART 3 OF THE DPA

Part 3 of the DPA transposed the Data Protection Law Enforcement Directive 2016/680 into local law. Part 3 of the DPA relates specifically to the protection of personal data when processed by Law Enforcement Authorities ("LEAs") for law enforcement purposes.

The standard of consent in Part 3 of the DPA is aligned with the GDPR. This Guidance Note thereby also serves to assist LEAs ensure that valid consent is obtained when it is being relied on to comply with Part 3 of the DPA.

IMPORTANT NOTE

This document is purely for guidance and aims to supplement the EDPB's Guidelines on consent under Regulation 2016/679[19]. The document does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the DPA will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions lies with the organisation.

Where necessary, the Information Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR and the DPA, the GDPR and the DPA will take precedence.

[19] See European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (Version 1.1) (4th May 2020).

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi