GIBRALTAR REGULATORY AUTHORITY

(19) COVID-19: Contact tracing and location data

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

29th April 2020

Guidance Note IR01/20

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

- The Commissioner notes the rapid developments in the use of technology to support the fight against COVID-19, in particular technology to 1) trace contact amongst the population, and 2) map the spread of the virus.

- As with any emerging technology, it is important to recognise the data protection and privacy risks that may arise from the use of technology. Data protection supports innovation by assuring the public that their data is protected.

Contact tracing framework

- Google and Apple are working on a joint initiative (the CTF) to provide a framework that others can use to develop contact tracing applications (the CTF is not itself an application).

- The Commissioner's UK counterpart i.e. the Information Commissioner's Office has carried out an assessment of the CTF and published its findings in a formal opinion. The Commissioner recognises the work carried out by the ICO, which considers that the CTF appears to be aligned with the principles of data protection by design and by default, data minimisation and security. Further, the application installation appears to be voluntary and the post-diagnosis upload of information to the application requires a separate consent process.

Contact tracing applications

- The data protection arrangements of the contact tracing applications themselves need to be considered separately to ensure that the application itself complies with data protection.

- The developer of a contact tracing application and body controlling the scheme will have data protection responsibilities that are additional and separate to those of frameworks such as the CTF.

- A Data Protection Impact Assessment must be carried out before implementing such tool as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution).

- Lawful basis - consent or a legislative measure would appear to be the most appropriate lawful grounds for contact tracing applications to comply with the requirements in the ePrivacy Regulations and the GDPR.

- Multiple actors typically exist within the mobile application ecosystem and each actor is likely to have separate data protection obligations. It is important that any data processing is conducted in a transparent manner to ensure that the user has ready access to clear information about who is processing their information and how.

Location data

- The two principal sources of location data available for modelling the spread are, 1) location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service; and 2) location data collected by the application.

- Lawful basis - the use of location data that is not anonymised is likely to require consent or a legislative measure to comply with the ePrivacy Regulations and the GDPR.

- When it comes to using location data, preference should always be given to the processing of anonymised data rather than personal data. However, anonymisation needs to be given careful consideration to ensure that it is effectively implemented.

- A DPIA must be carried out before implementing such tool as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution).

- The use of technology in the fight against COVID-19 is fast moving and complex. The Commissioner will remain engaged in this work, locally and internationally, and shall update its guidance as matters develop and where appropriate.

CONTENTS

1. ACKNOWLEDGEMENTS 1
2. INTRODUCTION 2
3. BACKGROUND 3
4. THE CTF & DATA PROTECTION COMPLIANCE 4
   4.1. DATA PROTECTION BY DESIGN AND BY DEFAULT 4
   4.2. DATA MINIMISATION 5
   4.3. USER CONTROL OVER APPLICATIONS BUILT USING THE CTF 5
   4.4. SECURITY 5
   4.5. PURPOSE LIMITATION AND RISKS OF SCOPE CREEP 6
   4.6. CURRENT ALIGNMENT WITH THE PROPOSED DP-3T SYSTEM 6
5. CONTACT TRACING APPLICATIONS 7
   5.1. ROLE OF APP DEVELOPER AND THE BODY CONTROLLING THE CONTACT TRACING SCHEME, AS CONTROLLER. 7
   5.2. DATA PROTECTION IMPACT ASSESSMENTS 8
   5.3. LAWFUL BASIS 8
   5.4. PURPOSE LIMITATION 9
   5.5. DATA MINIMISATION 9
   5.6. STORAGE LIMITATION 9
   5.7. PRIVACY INFORMATION, LAWFUL BASIS AND CONSENT MANAGEMENT 10
   5.8. SECURITY 10
   5.9. USER AWARENESS AND PERCEPTION 10
   5.10. SELF HELP QUESTIONS 11
6. LOCATION DATA 12
   6.1. SOURCES OF LOCATION DATA 12
   6.2. LAWFUL USE OF LOCATION DATA 12
   6.3. FOCUS ON THE USE OF ANONYMISED LOCATION DATA 13
   6.4. DATA PROTECTION IMPACT ASSESSMENTS 14
7. FURTHER DEVELOPMENTS 15

1. ACKNOWLEDGEMENTS

Where appropriate Gibraltar's Information Commissioner (the "Commissioner") will seek to ensure that locally published guidance notes replicate the guidance from the European Data Protection Board and/or are consistent with material published by fellow Information Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate material published by the UK Data Protection Authority.

(a) The UK's Information Commissioner's Office

'Blog: Combatting COVID-19 through data: some considerations for privacy'
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/

'Information Commissioner's Opinion: Apple and Google joint initiative on COVID-19 contact tracing technology'
https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

(b) The European Data Protection Board

'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak'
'https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en'

2. INTRODUCTION

The Gibraltar Regulatory Authority, as the Information Commissioner (the "Commissioner"), notes the rapid developments in the use of technology to contact trace amongst the population and map the spread of the virus, in support of the fight against COVID-19.

There is a possibility that contact tracing technology and/or location data may be deployed in Gibraltar in the fight against COVID-19. As with any emerging technology, it is important to recognise the data protection and privacy risks that may arise from the use of technology. It is important to note that data protection is not an obstacle to innovation and the development of technology; innovation and data protection are complimentary concepts. Data protection supports innovation by assuring the public that checks are in place to prevent the build-up of intrusive pictures of their lives. As with any new technology, its success depends on the public's confidence that it is being used in a fair and proportionate way.

In this guidance note, the Commissioner recognises an opinion published by his UK counterpart, the UK's Information Commissioner's Office (the "ICO"), in relation to a joint initiative by Apple and Google on COVID-19 contact tracing technology[1] (the "CTF"), and identifies key points from said opinion to serve as guidance on the CTF, including assurances of the same in relation to its compliance with data protection. This guidance note also provides guidance for the use of contact tracing applications and location data in the fight against COVID-19, taking into consideration guidance published by the European Data Protection Board ("EDPB").

The Commissioner's office is engaging with relevant parties, locally and internationally, to ensure that his office is able to offer help and guidance to projects looking to find innovative ways to help society whilst upholding the rights of individuals.

[1] https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

3. BACKGROUND

Contact tracing techniques seek to ascertain whether any individual has been in contact with an infected person during the time they were possibly infectious. Contact tracing could be used to support prompt communications with individuals who may be at risk of infection to ensure they -

1. are aware of the risk;
2. are provided with the appropriate information;
3. take the appropriate steps to protect themselves and others; and
4. receive any other support they may need.

Contact tracing has the potential to support measures to manage social distancing and may therefore enable any potential measures that would support the easing of lockdown or other restrictions.

Recently, there has been substantial focus on the possibility of supporting traditional contact tracing using automated tools, including the functionality available to many people on their mobile devices (e.g. their smart phone), as a means of addressing the COVID-19 pandemic. Said automated tools may therefore enable potential measures that would support the easing of lockdown or other restrictions.

Further to the use of automated tools for contact tracing, there is also focus on the use of location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures.

4. THE CTF & DATA PROTECTION COMPLIANCE

In regard to technological solutions using mobile phones, Google and Apple are working on a joint initiative i.e. the CTF, that will enable the development of contact tracing applications for use on mobile devices. A simple explanation of how an app is envisaged to work has been provided by Google and Apple.

The CTF is not itself a contact tracing application. The intention of the CTF is to provide a framework that others, for example public health authorities such as the Gibraltar Health Authority (the "GHA"), can use develop contact tracing applications that exchange information via Bluetooth Low Energy between devices.

The Commissioner's UK counterpart i.e. the ICO, has carried out an assessment of the CTF and published its findings in a formal opinion[2]. The Commissioner recognises the work carried out by the ICO and in the following outlines key points regarding the ICO's assessment.

4.1. DATA PROTECTION BY DESIGN AND BY DEFAULT

The CTF appears to be aligned with the principles of data protection by design and by default, including design principles around data minimisation and security. It is understood that the CTF is designed to –

1. only generate a limited amount of data from the user's device, that is then made available via the CTF application programming interface (API). This data includes periodically-generated cryptographic tokens (we have used the term 'tokens' for clarity, noting that the Apple and Google documentation calls these numbers 'identifiers') created on that device, and stored tokens collected from nearby devices via Bluetooth. Tokens are not associated with other data that may further identify or locate the device user; and
2. support the use of these tokens as part of a specific methodology for contact tracing, through their upload from a COVID-19 diagnosed user to a central server and subsequent notification to other app users from that server, with this process only matching tokens stored on a particular device (with the match only occurring on the device), if it had been in the proximity of the diagnosed user's device.

The CTF is therefore intended to support the development of applications that protect their users' identities, both before any risk of infection has been identified and when a COVID-19 infection notification is made via the app. However, it will be possible for those developing COVID-19 contact tracing applications (potentially to be whitelisted public health authorities and similar organisations) to design applications that use the CTF but also collect other data and use other techniques beyond those envisaged by the CTF.

[2] ICO, 'Opinion: Apple and Google joint initiative on COVID-19 contact tracing technology' (17 April 2020) < https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf > Accessed 17 April 2020

4.2. DATA MINIMISATION

The CTF appears to comply with the data minimisation principle. Based on an initial review -

1. The exchange of information between devices does not include personal data such as account information or usernames;
2. matching processes take place on-device and are not undertaken by the app host or with the involvement of any other third party; and
3. the information required for the core functionality of contact tracing applications built using CTF does not use location data, either in the exchange between devices, the upload to the app host or subsequent notifications to other users from the app host.

4.3. USER CONTROL OVER APPLICATIONS BUILT USING THE CTF

The app installation appears to be voluntary and the post-diagnosis upload of stored tokens to the app developer requires a separate consent process.

Any app built using the CTF will be provided via the applicable mobile Operating System (OS) app store and is subject to the same requirements as any other app within that app store. In addition, users have the ability to remove or disable the app. The user can also disable Bluetooth on their device.

However, it is understood that there will be a CTF 'Phase 2' where CTF API may form part of each mobile device's OS. This means that even a mobile device user who removes or disables an app will not be able to easily refuse or remove OS updates that continue to provide the CTF API, which enables applications to use this data.

4.4. SECURITY

The CTF documentation indicates the use of appropriate cryptographic functions with additional safeguards. Cryptographic techniques are a means of mitigating risks to the security of the data being processed, for example:

1. the generation of tokens takes place on the device and is not under the control of the contact tracing app utilising the API, using cryptographic techniques to ensure that information broadcast to other devices is not directly related to an identifiable individual. The exchange of tokens between devices do not indicate COVID-19 status, therefore the device-to-device level exchange of information does not directly result in app users knowing who has been diagnosed. While there may be circumstances where an individual could determine the identity of a diagnosed user (e.g. if they had only been in recent contact with a few people they know), these measures address risks about identification in circumstances such as public spaces;
2. if a user is diagnosed they can voluntarily upload the stored tokens on their device to the app host (e.g. the GHA) via an encrypted communications channel. The app host in turn lets other app users know that they may be at risk because they had recently been in close proximity to the diagnosed user, but this does not directly identify the diagnosed individual. While this is not intended to enable users to look up the tokens of COVID-19 positive users, the Commissioner understands that this may be possible, but only for a technically advanced attacker in specific circumstances, meaning this risk appears low;

3. the second-stage transfer of data to the app host is likely to be undertaken via transport layer security (TLS); and
4. no persistent user ID is broadcast. Instead, a sequence of pseudorandom tokens representing changing user IDs are broadcast. This means that the risk of identifying a user from the interaction between phone A and phone B in the moment is likely to be low.

4.5. PURPOSE LIMITATION AND RISKS OF SCOPE CREEP

Purpose limitation is a core data protection principle. It is about limiting use of personal data to the purpose for which it was collected or purposes compatible with that purpose. The CTF is a very new initiative and there are already signs that it will continue to evolve. Third-party app developers may also develop functionality that involves collection of additional data or new uses of existing data. This risks expanding the use of CTF-enabled applications beyond the stated purpose of contact tracing for COVID-19 pandemic response efforts. Developments shall be monitored with an eye to ensuring that this purpose does not expand outward, in the phenomenon known as scope creep.

4.6. CURRENT ALIGNMENT WITH THE PROPOSED DP-3T SYSTEM

The CTF is a joint initiative of Apple and Google and is not directly associated with the DP-3T initiative of a separate expert group. However, the underlying principles of the CTF appear to be similar to those proposed in the DP-3T protocol. However, this is subject to further developments and review.

5. CONTACT TRACING APPLICATIONS

As detailed in the forgoing, the CTF is a framework that is designed to enable the development of contact tracing applications and is not a contact tracing application in itself. The data protection arrangements of the contact tracing applications themselves need to be considered separately to ensure that the application itself complies with data protection. For example, the CTF does envisage the collection of location data, however application developers may add this data processing.

The following are key points that need to be considered in relation to contact tracing applications generally.

5.1. ROLE OF APP DEVELOPER AND THE BODY CONTROLLING THE CONTACT TRACING SCHEME, AS CONTROLLER.

The developer of a contact tracing application and body controlling the scheme will have data protection responsibilities that are additional and separate to those of frameworks such as the CTF.

Each controller designing an application is responsible for ensuring the app is compliant with data protection law and should adopt data protection by design and by default. The processing of additional data by applications that use frameworks such as the CTF is possible and may be legitimate and permissible. Where additional data processing takes place, a separate assessment of data protection considerations will need to be made by the controller, which may involve a separate data protection impact assessment ("DPIA").

To ensure accountability, the controller of any contact tracing application should be clearly defined. In Gibraltar, the GHA could be the controller. If the deployment of contact tracing applications involves different actors, their roles and responsibilities must be clearly established from the outset and be explained to the users.

Applications should adopt robust security (including the use of encryption, and covering each stage of the data processing), data minimisation, transparency and user control, and that any supporting technology, including centralised processing to support contact tracing, should follow the same principles.

Other key points to consider are:

1. In order to ensure their fairness, accountability and, more broadly, compliance with the law, algorithms must be auditable and should be regularly reviewed by independent experts. The application's source code should be made publicly available for the widest possible scrutiny.
2. Procedures and processes including respective algorithms implemented by the contact tracing applications should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives.

5.2. DATA PROTECTION IMPACT ASSESSMENTS

A DPIA must be carried out before implementing such tool as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution). The Commissioner strongly recommends the publication of DPIAs.

5.3. LAWFUL BASIS

The systematic and large-scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy. The EDPB has expressed its view that it can only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes i.e. consent. This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all.

It is important to note that contact tracing applications involve storage and/or access to information already stored in the terminal, which are subject to Regulation 5 of the Communications (personal data and privacy) Regulations 2006 (the "ePrivacy Regs"). To comply with Regulation 5 of the ePrivacy Regs, the application's storage and/or access to information stored in the terminal –

1. must be strictly necessary for the provider of the application to provide the service explicitly requested by the user; or
2. consent must be obtained[3].

In regard to compliance with the lawfulness of the processing under the GDPR, when public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Article 6(1)(e) of the GDPR. In this regard, it is important to note that Article 6(3) of the GDPR clarifies that the basis for the processing referred to in article 6(1)(e) of the GDPR shall be laid down in a law to which the controller is subject. Where legislation is introduced to provide the lawful basis for contact tracing, it is the Commissioner's view that the legislation should incorporate meaningful safeguards including:

1. A reference to the voluntary nature of the application.
2. A clear specification of purpose and explicit limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved.
3. The categories of data as well as the entities to (and purposes for which, the personal data may be disclosed) should also be identified. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing.
4. The criteria to determine when the application shall be dismantled and which entity shall be responsible and accountable for making that determination.

[3] The mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. If consent is relied on as the lawful grounds for processing, the controller shall ensure that the strict requirements relating to valid consent shall be complied with e.g. Article 7 of the GDPR.

It is important to note that the use of an application to fight the COVID-19 pandemic might lead to the collection of health data (for example the status of an infected person). Processing of such data is allowed when such processing is necessary for reasons of public interest in the area of public health, meeting the conditions of Article 9(2)(i) of the GDPR[4] or for health care purposes as described in Article 9(2)(h) of the GDPR. Depending on the legal basis, it might also be based on explicit consent (Article 9(2)(a) of the GDPR).

5.4. PURPOSE LIMITATION

With regard to the principle of purpose limitation, the purposes must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis (e.g., commercial or law enforcement purposes). Once the objective has been clearly defined, it will be necessary to ensure that the use of personal data is adequate, necessary and proportionate.

5.5. DATA MINIMISATION

In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default:

1. contact tracing applications do not require tracking the location of individual users. Instead, proximity data should be used;
2. as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification;
3. the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary; and
4. tracking should not occur by default – a user should not have to take action to prevent tracking.

The data processed should be reduced to the strict minimum. The application should not collect unrelated or not needed information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.

5.6. STORAGE LIMITATION

Storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period, etc.) and personal data should be kept only for the duration of the COVID-19 crisis. Afterwards, as a general rule, all personal data should be erased or anonymised. The current health crisis should not be used as an opportunity to establish disproportionate data retention mandates.

[4] The processing must be based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

5.7. PRIVACY INFORMATION, LAWFUL BASIS AND CONSENT MANAGEMENT

We must recognise that multiple actors typically exist within the mobile application ecosystem and that each actor is likely to have separate data protection obligations. It is important that any data processing is conducted in a transparent manner. Data controllers need to make sure that they comply with their transparency obligations under data protection law. This is particularly important when consent and explicit consent are relied on as the lawful basis for the data processing.

The Commissioner understands that most current proposals for contact tracing applications would rely on consent as the lawful basis for processing any personal data, and that installation of the applications is also voluntary. However, it is important to note that some matters remain unclear and must be addressed before being rolled out. For example –

1. it is not yet clear how the CTF will facilitate the collection of consent for the upload of stored tokens to the app host, although it is understood that the CTF will require the specific consent of the user at this point; and
2. it is not clear how an app utilising the CTF will manage this consent signal and how the CTF and an app may between them provide control to users. Last, it is unclear what impact consent withdrawal may have both on the effectiveness of contact tracing solutions and any notifications provided to other app users once an individual is diagnosed. Each of these matters will have to be addressed moving forward.

5.8. SECURITY

State-of-the-art cryptographic techniques must be implemented to secure the data stored in servers and applications, exchanges between applications and the remote server. Mutual authentication between the application and the server must also be performed.

The reporting of users as COVID-19 infected on the application must be subject to proper authorisation, for example through a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, no data processing should take place that presumes the validity of the user's status.

The controller, in collaboration with the public authorities, have to clearly and explicitly inform about the link to download the official national contact tracing app in order to mitigate the risk that individuals use a third-party app.

5.9. USER AWARENESS AND PERCEPTION

App developers or controllers should ensure their data processing is fair, lawful and transparent. Given the multiple actors involved in the mobile applications ecosystem, particular emphasis needs to be given on transparency to ensure that the user has ready access to clear information about who is processing their information and how. Use of the CTF as well as data being processed outside the scope of the CTF needs to be fair, lawful and transparent.

5.10. SELF HELP QUESTIONS

The following are a set of questions designed to help those developing technology to track and help fight COVID-19 –

1. *Have you demonstrated how privacy is built into the processor technology?*

The principles of data protection by design and by default are central to the law. Organisations want to move quickly but even an initial privacy impact assessment that is then developed is a minimum requirement.

2. *Is the planned collection and use of personal data necessary and proportionate?*

Technology can help address challenges prompted by this public health emergency, but thought needs to be given to finding the least privacy intrusive solutions.

This is especially important when 'location data' can mean many things. Some location data gives a more exact location than others. Some projects may be able to rely on data that is pseudonymised or anonymised to reduce the risk of reidentification. Conversations on proportionality must be informed by evidence.

3. *What control do users have over their data?*

People should be provided with clear information on how their information will be used, and their options for preventing processing where applicable. For instance, where contact tracing is being incorporated into a wider package of measures, this additional information would need to be clear.

4. *How much data needs to be gathered and processed centrally?*

The starting point for contact tracing should be decentralised systems that look to shift processing on to individuals' devices where possible. Safeguards and security measures need to accompany this, as well as any transfers of information.

5. *When in operation, what are the governance and accountability processes in your organisation for ongoing monitoring and evaluation of data processing – to ensure it remains necessary and effective, and to ensure that the safeguards in place are still suitable?*

Organisations need to ensure that their data processing is continuously under review with changes being made, as appropriate. This should be documented.

6. *What happens when the processing is no longer necessary?*

This is especially crucial: what is appropriate and proportionate in response to an international public health emergency looks quite different when that emergency ends. Consideration needs to be given to how and when data collection ends, and what happens to the data gathered.

6. LOCATION DATA

6.1. SOURCES OF LOCATION DATA

There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures:

1. location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service; and
2. location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.).

6.2. LAWFUL USE OF LOCATION DATA

It is important to note that location data collected from electronic communication providers may only be processed within the remits of the ePrivacy Regs, in particular Regulations 6, 7 and 15, which correspond to articles 6 and 9 of Directive 2002/58/EC (the "ePrivacy Directive"). This means that these data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users.

Regarding information, including location data, collected directly from the terminal equipment, Regulation 5 of the ePrivacy Regs applies, which corresponds to Article 5(3) of the ePrivacy Directive. Hence, the storing of information on the user's device or gaining access to the information already stored is allowed only if (i) the user has given consent or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user.

Derogations to the rights and obligations provided for in the ePrivacy Directive are however possible pursuant to Article 15 of the ePrivacy Directive, when they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives, including those referred to in Article 23(1) of the GDPR.

As for the re-use of location data collected by an information society service provider for modelling purposes (e.g. through the operating system or some previously installed application) additional conditions must be met. Indeed, when data have been collected in compliance with Regulation 5 of the ePrivacy Regs, they can only be further processed with the additional consent of the data subject or on the basis of a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR. Where legislation is introduced, in accordance with the ability to introduce national derogations, and/or to provide the lawful basis for the use of location data, it is the Commissioner's view that the legislation should incorporate meaningful safeguards including –

1. A clear specification of purpose and explicit limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved.
2. The categories of data as well as the entities to (and purposes for which, the personal data may be disclosed) should also be identified. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing.
3. The criteria to determine when the sharing/access of the data shall cease and be deleted, including which entity shall be responsible and accountable for making that determination.

The lawful basis relied on for the purposes of Article 6 of the GDPR will most likely correspond with the approach used under the ePrivacy Regs e.g. consent, performance of a task carried out in the public interest or legitimate interests.

In summary, the use of location data that is not anonymised is likely to require consent or a legislative measure.

6.3. FOCUS ON THE USE OF ANONYMISED LOCATION DATA

When it comes to using location data, **preference should always be given to the processing of anonymised data rather than personal data**. Anonymisation refers to the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any "reasonable" effort. Evaluating the robustness of anonymisation relies on three criteria: (i) singling-out (isolating an individual in a larger group based on the data); (ii) linkability (linking together two records concerning the same individual); and (iii) inference (deducing, with significant probability, unknown information about an individual).

It is important that anonymisation is given careful consideration to ensure that it is effectively implemented. Anonymisation processes and re-identification attacks are active fields of research. It is crucial for any controller implementing anonymisation solutions to monitor recent developments in this field, especially concerning location data (originating from telecom operators and/or information society services) which are known to be notoriously difficult to anonymise.

Research has shown[5] that location data thought to be anonymised may in fact not be. Mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances. A single data pattern tracing the location of an individual over a significant period of time cannot be fully anonymised. This assessment may still hold true if the precision of the recorded geographical coordinates is not sufficiently lowered, or if details of the track are removed and even if only the location of places where the data subject stays for substantial amounts of time are retained. This also holds for location data that is poorly aggregated.

Given the complexity of anonymisation processes, transparency regarding the anonymisation methodology is highly encouraged.

[5] (de Montjoye et al., 2013) "Unique in the Crowd: The privacy bounds of human mobility" and (Pyrgelis et al., 2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data

6.4. DATA PROTECTION IMPACT ASSESSMENTS

If personal data is processed, a DPIA must be carried out before the data processing takes place as the processing is considered likely high risk (anticipated large-scale adoption, systematic monitoring, use of new technological solution). The Commissioner strongly recommends the publication of DPIAs.

7. FURTHER DEVELOPMENTS

The use of technology in the fight against COVID-19 is fast moving and complex. The Commissioner will remain engaged in this work, locally and internationally, and shall update its guidance as matters develop and where appropriate.

IMPORTANT NOTE

This document is purely for guidance and 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 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.

CONTACT US

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

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