GRA

GIBRALTAR REGULATORY AUTHORITY

(6) Identifying the 'Lawful Basis'

Guidance on the General Data Protection Regulation

30 August 2018

Guidance Note IR01/18

CONTENTS

SUMMARY

The General Data Protection Regulation and the Data Protection Act 2004 list the lawful bases that organisations can rely on to process personal data legitimately, depending on the 'category' of personal data. This Guidance Note aims to identify the lawful bases that are available for organisations to rely on, for each category, in a practical and concise manner.

Lawful bases for personal data

1. Consent.
2. Contract.
3. Legal obligation.
4. Vital interests.
5. Public task–
   (a) justice;
   (b) parliament;
   (c) statutory function; or
   (d) Minister or Gov. Dept.
6. Legitimate interests.

Lawful bases for special categories of personal data

1. Explicit consent.
2. Employment, social security and social protection.
3. Vital interests.
4. Not for profit use.
5. Public data.
6. Legal proceedings.
7. Health or social care purposes –
   (a) preventative or occupational medicine;
   (b) assessment of the working capacity of employee;
   (c) medical diagnosis;
   (d) provision of health care or treatment;
   (e) the provision of social care;
   (f) the Mangt. of health/social care systems; or
   (g) medical research.
8. Public health.
9. Research.
10. Substantial public interest –
    (a) statutory function;
    (b) Minister or a Gov. Dept.;
    (c) justice;
    (d) parliament;
    (e) equality;
    (f) racial & ethnic diversity;
    (g) preventing or detecting unlawful acts;
    (h) protecting the public against dishonesty;
    (i) regulatory compliance or assisting with compliance;
    (j) journalism;
    (k) preventing fraud;
    (l) preventing terrorist financing or money laundering;
    (m) supporting individuals with particular disabilities or medical conditions;
    (n) counselling;
    (o) safeguarding children;
    (p) safeguarding economic well-being of individuals;
    (q) insurance;
    (r) occupational pensions;
    (s) political party;
    (t) elected representative responding to requests;
    (u) disclosures to elected representatives;
    (v) informing elected representatives about prisoners;
    (w) publication of legal judgements;
    (x) anti-doping in sport; or
    (y) sports integrity;

Lawful bases for data relating to criminal convictions and offences

1. Consent.
2. Employment, social security and social protection.
3. Vital interests.
4. Not for profit use.
5. Public data.
6. Legal proceedings.
7. Health or social care purposes –
   (a) preventative or occupational medicine;
   (b) the assessment of the working capacity of an employee;
   (c) medical diagnosis;
   (d) the provision of health care or treatment;
   (e) the provision of social care;
   (f) the Mangt. of health/social care systems; or
   (g) medical research.
8. Public health.
9. Research.
10. Judicial acts.
11. Administering commission of offences relating to indecency.
12. Substantial public interest –
    (a) statutory function;
    (b) Minister or a Gov. Dept.;
    (c) justice;
    (d) parliament;
    (e) equality;
    (f) racial & ethnic diversity;
    (g) preventing or detecting unlawful acts;
    (h) protecting the public against dishonesty;
    (i) regulatory compliance or assisting with compliance;
    (j) journalism;
    (k) preventing fraud;
    (l) preventing terrorist financing or money laundering;
    (m) supporting individuals with particular disabilities or medical conditions;
    (n) counselling;
    (o) safeguarding children;
    (p) safeguarding economic well-being of individuals;
    (q) insurance;
    (r) occupational pensions;
    (s) political party;
    (t) elected representative responding to requests;
    (u) disclosures to elected representatives;
    (v) informing elected representatives about prisoners;
    (w) publication of legal judgements;
    (x) anti-doping in sport; or
    (y) sports integrity;
13. Substantial public interest (extension)
14. Insurance (extension)

1. INTRODUCTION

To process personal data legitimately under the General Data Protection Regulation ("GDPR") and the Data Protection Act 2004 ("DPA") organisations need to have a 'lawful basis'. Identifying the lawful basis that an organisation relies on to process personal data is a fundamental step in ensuring data protection compliance.

The GDPR and the DPA list the lawful bases that organisations can rely on, depending on the 'category' of personal data i.e. whether the information is 'personal data', 'a special category of personal data' or 'data relating to criminal convictions and offences'. This Guidance Note aims to identify the lawful bases that are available for organisations to rely on, for each category, in a practical and concise manner.

The information provided should be treated as guidance with appropriate consideration being given to the actual legal requirements. Footnotes referencing the legislation are included so that readers are able to link and relate the guidance to the specific provisions in the law.

2. GENERAL GUIDANCE

- The lawful basis that is most appropriate to use will depend on the circumstances of the organisation and purposes of the processing.

- Most lawful bases require that processing is 'necessary'. In these cases, the lawful basis cannot be relied on when an organisation can reasonably achieve the same purpose without the processing.

- Organisations must identify and document its lawful basis, including the reasoning for relying on the lawful basis identified, before it begins collecting and using personal data. This is important and useful as the accountability principle[1] requires organisations to be able to demonstrate compliance. It is also important and necessary for the transparency requirements, which oblige organisations to inform individuals upfront about the lawful basis that they rely on to process their information[2].

- Organisations may find that more than one lawful basis could apply in a particular case. If so, the organisation may identify and document all of them. In some cases, more than one basis applies to the processing because the processing has more than one purpose, and if this is the case this should be identified from the start.

- If a public authority can demonstrate that the processing is to perform tasks as set down in Gibraltar law, then it will be able to use the public task basis. If not, it may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and its relationship with individuals. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the GDPR does restrict public authorities' use of these two bases.

[1] Article 5(2) of the GDPR

[2] Article 13(1)(c) of the GDPR

3. THE THREE CATEGORIES OF PERSONAL DATA

The law differentiates between 'personal data', 'special categories of personal data' and 'data relating to criminal convictions and offences'.

- Personal data - in summary, if you can associate information with an individual, it is personal data. e.g. name, address, IP, telephone number, physical characteristics, life history, location data, etc… The law defines personal data as follows –

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Within the broad definition of personal data, the law gives a distinctive status to certain types of personal data, which are defined as 'special categories of personal data' and 'data relating to criminal convictions'. Both categories are considered more sensitive, require greater protection and can only be processed in more limited circumstances.

- Special categories of personal data – defined in law as follows –

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- Data relating to criminal convictions and offences – defined simply as data relating to criminal convictions and offences or related security measures.

4. PERSONAL DATA

The lawful bases that organisations can rely on to process personal data are the following –

4.1. Consent[3]: the individual has given clear consent to process their personal data for a specific purpose.

4.2. Contract[4]: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

4.3. Legal obligation[5]: the processing is necessary for you to comply with the law (not including contractual obligations).

[3] Article 6(1)(a) of the GDPR

[4] Article 6(1)(b) of the GDPR

[5] Article 6(1)(c) of the GDPR

4.4. Vital interests[6]: the processing is necessary to protect someone's life.

4.5. Public task[7]: the processing is necessary for –
   4.5.1. the administration of justice[8];
   4.5.2. the exercise of a function of parliament[9];
   4.5.3. the exercise of a function conferred on a person by an enactment or rule of law[10]; or
   4.5.4. the exercise of a function of a Minister or a government department[11].

4.6. Legitimate interests[12]: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

5. SPECIAL CATEGORIES OF PERSONAL DATA

When an organisation collects and uses a special category of personal data, it must identify both a lawful basis in the foregoing paragraph 4 and one of the following:

5.1. Explicit consent[13]: the individual has given explicit consent to the processing of those personal data for one or more specified purposes.

5.2. Employment, social security and social protection[14]: the information is necessary for one of the following[15] –
   5.2.1. performing obligations imposed on the organisation in connection with employment, social security or social protection; or
   5.2.2. exercising the rights of an individual in connection with employment, social security or social protection.

5.3. Vital interests[16]: the processing is necessary to protect the life of the individual when they are physically or legally incapable of giving consent.

5.4. Not for profit use[17]: the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who

---

[6] Article 6(1)(d) of the GDPR
[7] Article 6(1)(e) of the GDPR
[8] Section 10(a) of the DPA
[9] Section 10(b) of the DPA
[10] Section 10(c) of the DPA
[11] Section 10(d) of the DPA
[12] Article 6(1)(f) of the GDPR
[13] Article 9(2)(a) of the GDPR
[14] Article 9(2)(b) of the GDPR
[15] Schedule 1, part 1, paragraph 1(1) of the DPA
[16] Article 9(2)(c) of the GDPR
[17] Article 9(2)(d) of the GDPR

have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the individuals.

5.5. Public data[18]: the personal data is information that was manifestly made public by the individual.

5.6. Legal proceedings[19]: the data is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

5.7. Health or social care purposes[20]: the information is necessary for one of the following –
- 5.7.1. preventative or occupational medicine;
- 5.7.2. the assessment of the working capacity of an employee;
- 5.7.3. medical diagnosis;
- 5.7.4. the provision of health care or treatment;
- 5.7.5. the provision of social care;
- 5.7.6. the management of health care systems or services or social care systems or services; or
- 5.7.7. medical research.

It is important to note that reliance on the above are subject to obligations of secrecy[21].

5.8. Public health[22]: the information is necessary for reasons of of public interest in the area of public health and is carried out by or under the responsibility of a health professional, or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

5.9. Research[23]: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and is carried out in accordance with Article 89(1) of the GDPR.

5.10. Substantial public interest[24]: the processing is necessary for one of the following –
- 5.10.1. the exercise of a function conferred on a person by an enactment or rule of law and for reasons of substantial public interest[25];
- 5.10.2. the exercise of a function of a Minister or a government department for reasons of substantial public interest[26];
- 5.10.3. the administration of justice[27];
- 5.10.4. the exercise of a function of parliament[28];
- 5.10.5. equality of opportunity or treatment[29];
- 5.10.6. promoting or maintaining racial and ethnic diversity at senior levels of organisations[30];
- 5.10.7. preventing or detecting unlawful acts[31];
- 5.10.8. protecting the public against dishonesty[32];

---

[18] Article 9(2)(e) of the GDPR
[19] Article 9(2)(f) of the GDPR
[20] Article 9(2)(h) of the GDPR and schedule 1, part 1, paragraph 2 of the DPA
[21] Section 13(1) of the DPA
[22] Article 9(2)(i) of the GDPR and schedule 1, part 1, paragraph 3 of the DPA
[23] Article 9(2)(j) of the GDPR and schedule 1, part 1, paragraph 4 of the DPA
[24] Article 9(2)(g) of the GDPR and section 12(3) of the DPA and schedule 1, part 2 of the DPA
[25] Schedule 1, part 2, paragraph 6 of the DPA
[26] Schedule 1, part 2, paragraph 6 of the DPA
[27] Schedule 1, part 2, paragraph 7 of the DPA
[28] Schedule 1, part 2, paragraph 7 of the DPA
[29] Schedule 1, part 2, paragraph 8 of the DPA
[30] Schedule 1, part 2, paragraph 9 of the DPA
[31] Schedule 1, part 2, paragraph 10 of the DPA
[32] Schedule 1, part 2, paragraph 11 of the DPA

5.10.9. complying with, or assisting other persons, to comply with a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct[33];
5.10.10. journalism etc in connection with unlawful acts and dishonesty etc. [34];
5.10.11. preventing fraud[35];
5.10.12. preventing terrorist financing or money laundering[36];
5.10.13. supporting individuals with particular disabilities or medical conditions[37];
5.10.14. counselling[38];
5.10.15. safeguarding of children and of individuals at risk[39];
5.10.16. safeguarding of economic well-being of certain individuals[40];
5.10.17. insurance purposes[41];
5.10.18. administering occupational pensions[42];
5.10.19. the activities of a political party[43];
5.10.20. an elected representative responding to requests[44];
5.10.21. disclosure to elected representatives[45];
5.10.22. inform elected representatives about prisoners[46];
5.10.23. publication of legal judgements[47];
5.10.24. anti-doping in sport[48]; or
5.10.25. sports integrity[49];

Note that to rely on any of the grounds listed above under paragraph 5.10, the organisation must have an appropriate policy document in place as per schedule 1, part 4, paragraph 39 of the DPA[50]. Only in certain circumstances relating to anti-doping in sport, journalism, and preventing or detecting unlawful acts, does this requirement not apply.

[33] Schedule 1, part 2, paragraph 12 of the DPA
[34] Schedule 1, part 2, paragraph 13 of the DPA
[35] Schedule 1, part 2, paragraph 14 of the DPA
[36] Schedule 1, part 2, paragraph 15 of the DPA
[37] Schedule 1, part 2, paragraph 16 of the DPA
[38] Schedule 1, part 2, paragraph 17 of the DPA
[39] Schedule 1, part 2, paragraph 18 of the DPA
[40] Schedule 1, part 2, paragraph 19 of the DPA
[41] Schedule 1, part 2, paragraph 20 of the DPA
[42] Schedule 1, part 2, paragraph 21 of the DPA
[43] Schedule 1, part 2, paragraph 22 of the DPA
[44] Schedule 1, part 2, paragraph 23 of the DPA
[45] Schedule 1, part 2, paragraph 24 of the DPA
[46] Schedule 1, part 2, paragraph 25 of the DPA
[47] Schedule 1, part 2, paragraph 26 of the DPA
[48] Schedule 1, part 2, paragraph 27 of the DPA
[49] Schedule 1, part 2, paragraph 28 of the DPA
[50] Schedule 1, part 2, paragraph 5 of the DPA

6. DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

When an organisation processes personal data relating to criminal convictions and offences, it must identify both a lawful basis in the foregoing paragraph 4 and one of the following[51]:

6.1. Any of the grounds in paragraphs 5.2, 5.7, 5.8, 5.9, and 5.10 identified in the foregoing.

6.2. Consent[52]: the individual has given his consent.

6.3. Protecting the individual's vital interests[53]: the processing is necessary to protect the life of the individual when they are physically or legally incapable of giving consent.

6.4. Activities by not for profit bodies[54]: the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the individuals.

6.5. Public data[55]: the personal data is information that was manifestly made public by the individual.

6.6. Legal claims[56]: the processing is necessary for, or in connection with legal proceedings, for the purposes of obtainin legal advice or otherwise necessary for establishing or defending legal rights.

6.7. Judicial acts[57]: processing by a court or tribunal in their judicial capacity.

6.8. Administration of accounts used in commission of indecency offences involving children[58]: the processing is of personal data about a conviction or caution for an offence relating to indecent photographs of children.

6.9. Substantial public interest (extension): the grounds in paragraph 5.10, without meeting the "substantial public interest" test.

6.10. Insurance (extension): extends the grounds in sub-paragraph 5.10.17 to the processing of personal data not revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, for insurance purposes, with or without meeting the "substantial public interest" test.

---

[51] Section 12(5) of the DPA

[52] Schedule 1, part 3, paragraph 29 of the DPA

[53] Schedule 1, part 3, paragraph 30 of the DPA

[54] Schedule 1, part 3, paragraph 31 of the DPA

[55] Schedule 1, part 3, paragraph 32 of the DPA

[56] Schedule 1, part 3, paragraph 33 of the DPA

[57] Schedule 1, part 3, paragraph 34 of the DPA

[58] Schedule 1, part 3, paragraph 35 of the DPA

7. GRAPHICAL ILLUSTRATION OF LAWFUL BASES

The following charts illustrate the lawful bases that organisations can rely on to process personal data, specific categories of personal data and data relating to criminal convictions or offences. as identified in the foregoing.

*CHART 1 – LAWFUL BASES TO PROCESS **PERSONAL DATA***

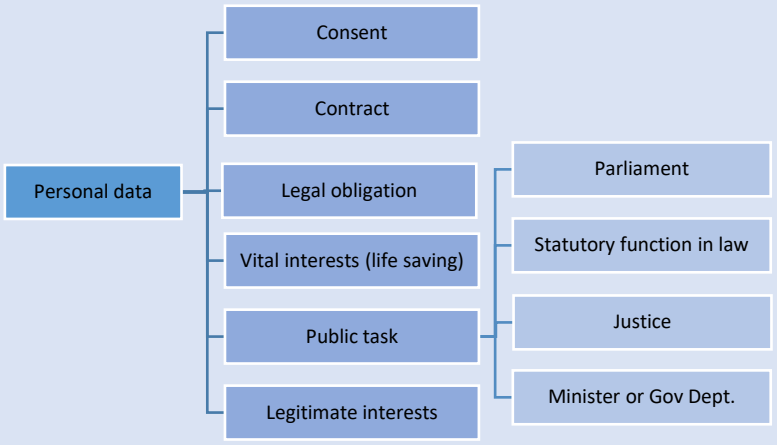


CHART 2 – LAWFUL BASES TO PROCESS ***SPECIAL CATEGORIES OF PERSONAL DATA***

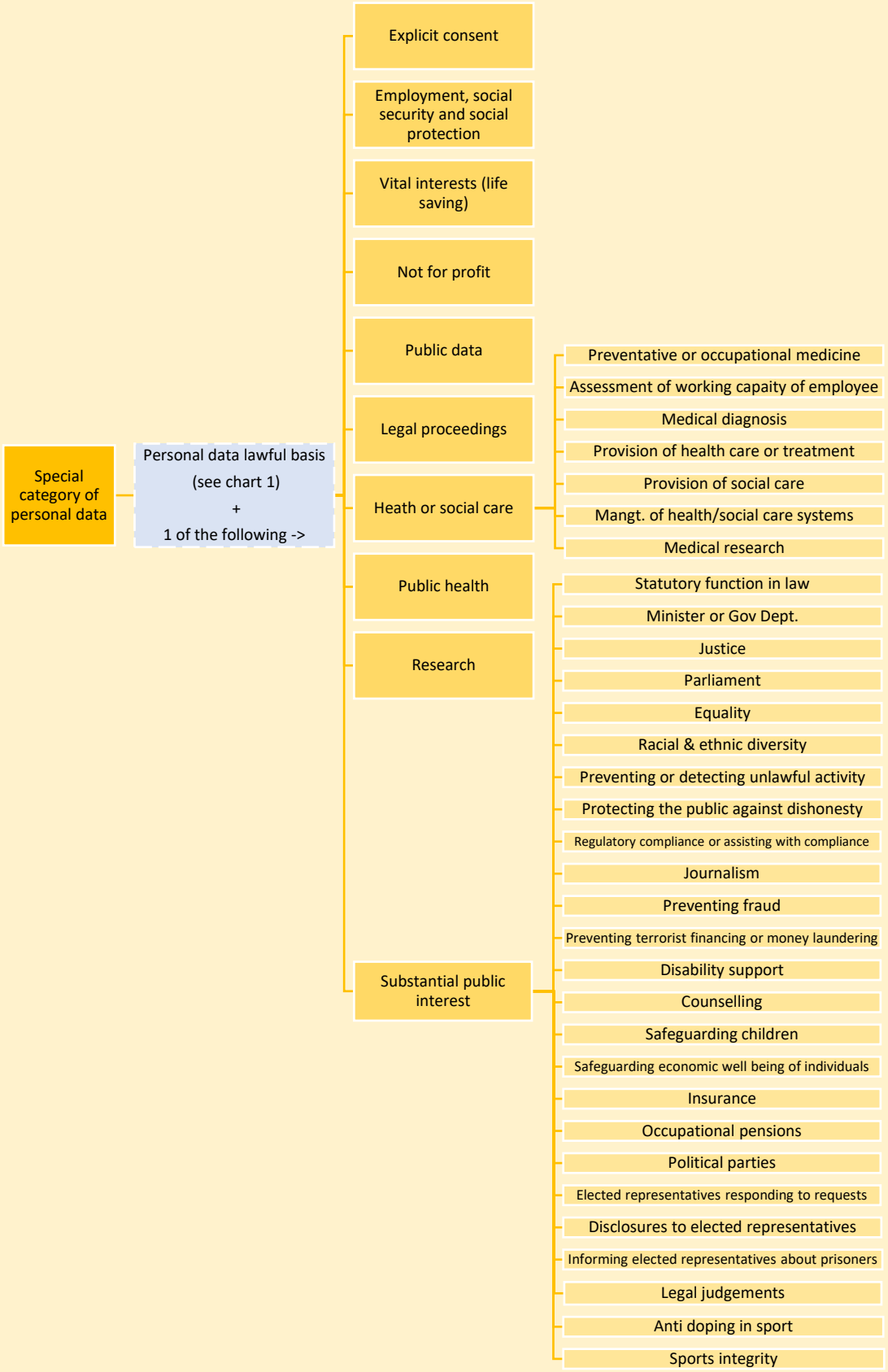
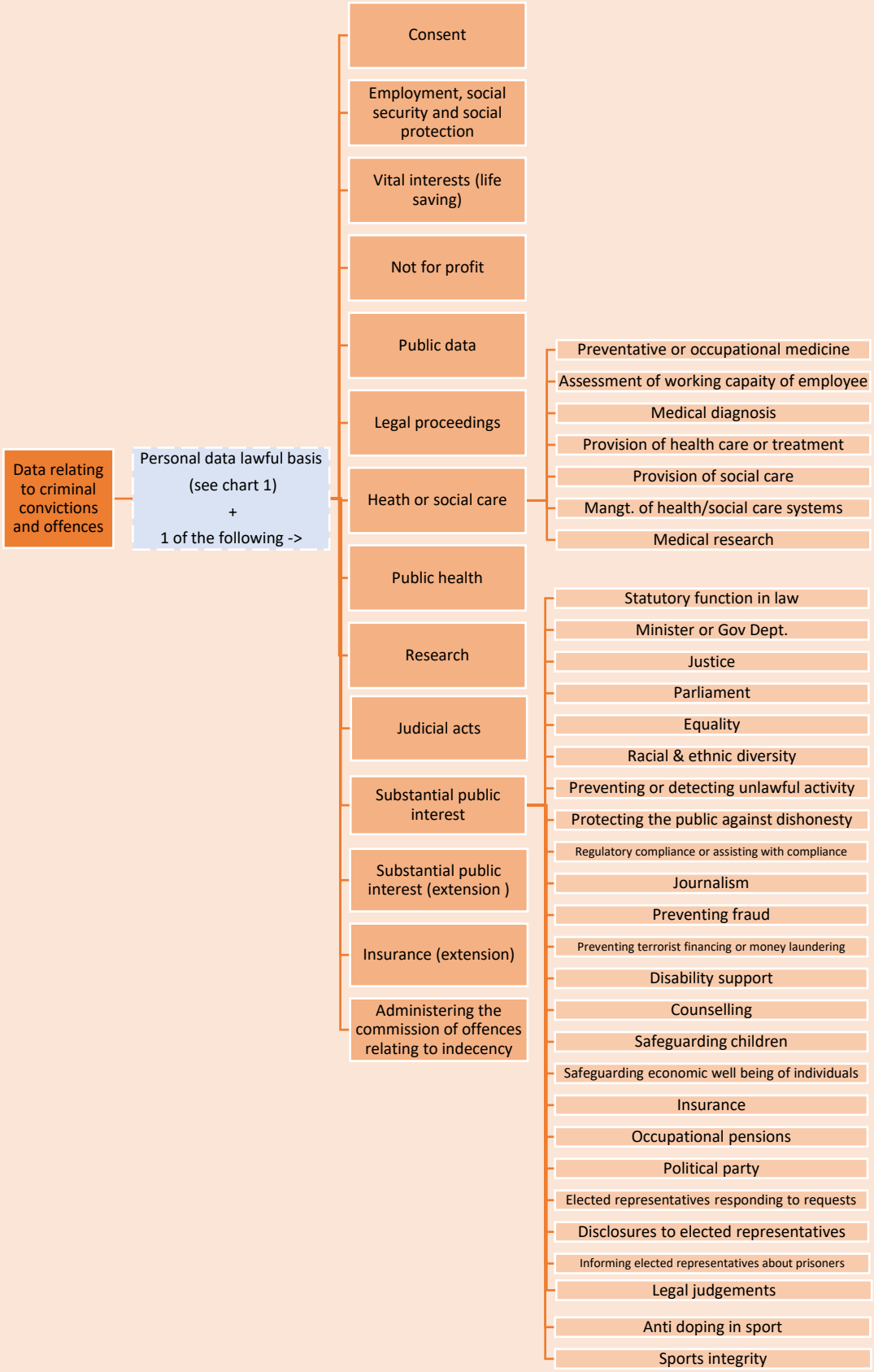


CHART 3 – LAWFUL BASES TO PROCESS ***DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES***



IMPORTANT NOTE

This document is purely for guidance. The document does not constitute legal advice or legal analysis. All organisations that process data need to be aware that the GDPR 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 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