**Complaint**

**to the commission of the european union**

**concerning the failure to comply with EU law**

**by**

**the united Kingdom**

**in connection with the UK Rules on Data Protection**

[I. IDENTITY AND CONTACT DETAILS OF COMPLAINANT AND THEIR REPRESENTATIVE 2](#_Toc10494460)

[1. Representative’s contact details 2](#_Toc10494461)

[2. I am submitting this complaint on behalf of someone else: 2](#_Toc10494462)

[3. Correspondence from the Commission can be sent to the complainant or the complainant’s representative 2](#_Toc10494463)

[II. DESCRIPTION OF THE SUSPECTED INFRINGEMENT OF UNION LAW 3](#_Toc10494464)

[4. Description of the facts and the reasons for your complaint and remedial action sought 3](#_Toc10494465)

[UK Data Protection Act 2018 3](#_Toc10494466)

[The EU General Data Protection Regulation 3](#_Toc10494467)

[Article 23 provides a limited basis for limiting application of the GDPR 4](#_Toc10494468)

[The “immigration control exemption” is incompatible with the GDPR 4](#_Toc10494469)

[The “immigration control exemption” does not safeguard a specific and important public interest of the kind envisioned by Article 23, and is not justified based on a “pressing social need” 5](#_Toc10494470)

[The “immigration control exemption” is overbroad, and neither clear nor precise enough to be foreseeable for affected individuals 7](#_Toc10494471)

[Derogations from data subject rights under the “immigration control exemption” are neither necessary nor proportionate 8](#_Toc10494472)

[In the context of the UK’s current “hostile environment”, the “immigration control exemption” risks supporting further violations of the fundamental rights and freedoms of affected individuals 11](#_Toc10494473)

[The “immigration control exemption” fails to establish the safeguards required under Article 23(2) GDPR 14](#_Toc10494474)

[Conclusion 15](#_Toc10494475)

[5. Does your complaint relate to the EU Charter of Fundamental Rights, which applies only to the implementation of Union law (Article 51)? 16](#_Toc10494476)

[6. If possible, please provide a list of documents or evidence in support of your complaint (including the national measures concerned) that you can send to the Commission if it so requests: 17](#_Toc10494477)

[III. APPEALS / LEGAL ACTIONS / OTHER ACTIONS 17](#_Toc10494478)

# **IDENTITY AND CONTACT DETAILS OF COMPLAINANT AND THEIR REPRESENTATIVE**

## Representative’s contact details

Name of organisation: Platform for International Cooperation on Undocumented Migrants

(PICUM)

Name and Surname of legal representative: Michele LeVoy, Director, PICUM

Address: 37-41 rue du Congrès

Town: Brussels

Postcode: 1030

Country: BELGIUM

Telephone: + 32 2 210 1780

Fax: +32 2 210 1789

E-mail: [alyna.smith@picum.org](mailto:alyna.smith@picum.org)

## I am submitting this complaint on behalf of someone else:

Yes ( ) No ( X )

## Correspondence from the Commission can be sent to the complainant or the complainant’s representative

Complainant ( ) Representative ( X )

# DESCRIPTION OF THE SUSPECTED INFRINGEMENT OF UNION LAW

## Description of the facts and the reasons for your complaint and remedial action sought

1. Description of the facts:

#### UK Data Protection Act 2018

The United Kingdom’s Data Protection Act 2018 (“DPA”) updates the data protection laws in the UK and is intended to complement the EU General Data Protection Regulation (EU) 2016/679 (“GDPR”), which has direct effect in all EU member states. The DPA received Royal Assent on 23 May 2018 and went into effect on 25 May 2018.

This complaint addresses Schedule 2, Part 1, paragraph 4 of the DPA, which creates a broad exemption (hereinafter “immigration control exemption” or “exemption”) to the application of GDPR protections, based on the limited basis provided for derogations under GDPR Article 23. It is our submission that the “immigration control exemption” does not comport with Article 23, and is therefore a violation of the GDPR, as well as rights guaranteed under the EU Charter of Fundamental Rights (“Charter” or “CFR”) and European Convention on Human Rights (“ECHR”).

#### *The EU General Data Protection Regulation*

The GDPR strengthens and implements fundamental human rights to privacy and data protection. Like the Data Protection Directive before it, GDPR is steeped in the traditions of the ECHR,[[1]](#footnote-1) the Council of Europe’s Convention no. 108 (1981),[[2]](#footnote-2) and the OECD guidelines of 1980.[[3]](#footnote-3) These rights have their historical origins among others in the reaction to the atrocities of World War II and the privacy rights infringements prevalent in socialist regimes in Eastern Europe during the Cold War.

More recently, the 2007 Lisbon Treaty[[4]](#footnote-4) established in its Article 6(1) that the Charter has the same legal value as the EU treaties and in its Article 6(3) that the fundamental rights enshrined in the ECHR constitute general principles of European Union law. Article 8(2) of the Charter elevates the protection of personal data to a specific and distinct fundamental right in the EU and provides that processing of personal data is in principle prohibited unless based on the consent of the data subject or a legitimate basis found in the law.

The importance in the EU legal order of the fundamental right to privacy (Article 7 of the Charter) and the protection of personal data (Article 8 of the Charter) has been repeatedly emphasized by the Court of Justice of the European Union (CJEU).[[5]](#footnote-5) These principles are also deeply embedded in the constitutional legal orders of most (if not all) EU member states.

In that context, GDPR must be understood as an effort to strengthen even further those fundamental rights, taking into account the advancement of technology and the ease with which personal data can be collected and transmitted today. The provisions of GDPR must therefore be read and interpreted in light of these other legal instruments protecting the same fundamental right to data protection and the jurisprudence developed by the CJEU and the European Court of Human Rights.[[6]](#footnote-6)

#### Article 23 provides a limited basis for limiting application of the GDPR

Article 23 GDPR offers EU member states a legal basis to create limited exceptions to certain of the GDPR’s protections. Any measure taken under Article 23 must, however, meet a number of strict conditions and must be compatible with fundamental rights enshrined in the ECHR and the Charter. Namely, Article 23(1) GDPR requires that any such measure:

1. is aimed at safeguarding a specific and important public interest, such as national security or public security;
2. is sufficiently clear and precise to be foreseeable for affected individuals;
3. is necessary and proportionate in a democratic society; and
4. respects the essence of the fundamental rights and freedoms of affected individuals, including their right to data protection.

These requirements are consistent with the jurisprudence of the European Court of Human Rights.[[7]](#footnote-7) Although governments enjoy a margin of discretion to restrict privacy rights, this margin is more limited when information of a very private nature or fundamental rights of data subjects are at stake.[[8]](#footnote-8) In addition, measures adopted under Article 23 GDPR must be interpreted restrictively and narrowly to the extent they constitute deviations from fundamental data protection principles enshrined in GDPR.[[9]](#footnote-9)

#### The “immigration control exemption” is incompatible with the GDPR

The “immigration control exemption” created under paragraph 4 of Schedule 2, Part 1 of the DPA is justified on the basis of Articles 23(1) of the GDPR. It sets out that:

4 (1) The GDPR provisions listed in sub-paragraph (2) do not apply to personal data for any of the following purposes –

1. the maintenance of effective immigration control, or
2. the investigation or detection of activities that would undermine the maintenance of effective immigration control

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b).

Under sub-paragraph (2), the exemption derogates from several data subject rights namely the right to information about the processing of one’s data (whether it was obtained from the data subject (Art. 13(1)-(3) GDPR) or from another source (Art. 14(1)-(4) GDPR)); the right to access one’s data (including the right to get confirmation about whether one’s data is being processed and for what purpose) (Art. 15(1)-(3) GDPR); the right to erasure (Art. 17(1)-(2) GDPR); the right to restrict the processing of one’s data (Article 18(1) GDPR); and the right to object to the processing of one’s data, on any ground and at any time (Article 21(1) GDPR).

In addition, the exemption restricts application of the data protection principles, set out under Article 5 of GDPR, of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability, to the extent that they correspond to the rights mentioned above.

Significantly, under Schedule 2, Part 1, sub.-para. 4(3), the “immigration control exemption” applies both when data is initially processed (such as, by a service provider), and when it is further processed by a separate person or entity (such as the Home Office) for maintaining effective immigration control or investigating or detecting activities that would undermine immigration control.

#### The “immigration control exemption” does not safeguard a specific and important public interest of the kind envisioned by Article 23, and is not justified based on a “pressing social need”

Exemptions to the GDPR must aim at “safeguarding specific and important public interests” (emphasis added). The “maintenance of effective immigration control” and the “investigation or detection of activities that would undermine the maintenance of effective immigration control” – the purposes for the claimed exemption under Schedule 2, Part I, paragraph 4 – are neither specific nor do they constitute important public interests of the kind foreseen by the GDPR.

It is instructive to consider other exemptions under Schedule 2 of the DPA. Besides the “immigration control exemption”, Schedule 2, Part 1 of the DPA creates exemptions for crime and taxation (sub-paragraphs 2 and 3), and the disclosure of information in the context of legal proceedings (sub-paragraph 5). Schedule 2, Part 2 regulates exemptions related to a host of functions, many of which are concerned with oversight mechanism to address financial fraud and malpractice or misconduct by public bodies and corporations. Others concern exemptions related to the functions of statutory bodies that carry out audits and of the Bank of England, and that hear complaints from the public, such ombudspersons and commissioners. There are provisions exempting application of certain articles of the GDPR in the context of parliamentary privilege, judicial appointments and independence, legal privilege, self-incrimination, for reasons of freedom of expression and information, for research, statistics and archiving, and for health, social work, education and child abuse.

These exemptions are, on their face, in keeping with the list in Article 23(1)(i) of functions that constitute an “important public interest”. “Immigration control” stands as an outlier, with no clear home among the enumerated functions that meet this high threshold:

1. national security;
2. defence;
3. public security;
4. the prevention, investigation, detection or prosecution of criminal offense or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
5. other important objectives of general public interest of the Union or a of a Member States, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
6. the protection of judicial independence and judicial proceedings;
7. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
8. monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
9. the protection of the data subject or the rights and freedoms of others;
10. the enforcement of civil law claims.

There is no plausible basis for characterising “immigration enforcement” as either a matter of “national security” or “defence”; and it clearly falls outside the purview of the functions enumerated in sub-paragraphs (d) through (j). What remains is “public security” as a basis for limiting the reach of the GDPR in this context. However, “public security” is itself a very narrow concept, which has been summarised this way in the proposed EU regulation on the free flow of non-personal data, recently adopted by the European Parliament:

The concept of ‘public security’, within the meaning of Article 52 of the TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in particular to allow for the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services, and the survival of the population, as well as by the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests.[[10]](#footnote-10) (emphasis added)

It is natural that the threshold for deviating from the GDPR is high. The requirements of Article 23 are consistent with the jurisprudence of the European Court of Human Rights, which limits governments’ margin of discretion to restrict privacy rights, when information of a private nature or the fundamental rights of data subjects are at stake.[[11]](#footnote-11) Measures infringing privacy and data protection rights in such contexts must be justified by a “*pressing social need*” and must be “*balanced against the seriousness of the interference*” with the affected individuals’ fundamental rights.[[12]](#footnote-12) Member states do not have unfettered discretion in carving out exceptions to the GDPR.

The enforcement of immigration laws cannot reasonably be said to meet the threshold of “pressing social need”, particularly (as will be seen below) given the fundamental rights at stake, including but not limited to data protection. Treating “immigration enforcement” as an important public interest, akin to national or public security, would stretch the application of Article 23(1) beyond its intended narrow scope, creating a wide category of individuals who potentially fall outside GDPR protections because of unclear distinctions based on their residence status or purported immigration law offences, and exposing them to substantial violations of their fundamental rights.

#### The “immigration control exemption” is overbroad, and neither clear nor precise enough to be foreseeable for affected individuals

The “immigration exemption” creates a sweeping exception to the protections of the GDPR, falling well short of the requirement under Article 23 that measures be clear and precise enough to be foreseeable for affected individuals.

The stated purposes of the “immigration control exemption” are:

1. the maintenance of effective immigration control, and
2. the investigation or detection of activities that would undermine the maintenance of effective immigration control

Nowhere in the DPA, however, are the terms “effective” or “immigration control” defined. The exemption is therefore both incredibly broad in its scope and incredibly vague, giving data controllers wide latitude in restricting important rights. This vagueness is particularly problematic given the volume and complexity of immigration law in the UK. Legislative provisions underlying immigration law are scattered throughout Acts of Parliament from 1971, 1988, 1999, 2002, 2004, 2006, 2007, 2008, 2009, 2014 and 2016, all of which contain applicable provisions, while also amending previous legislation.[[13]](#footnote-13) One UK jurist remarked in Sapkota v. Secretary of State for the Home Department [2011] EWCA Civ 1320:

I regret that this area of immigration law has now become an impenetrable jungle of intertwined statutory decisions, with the result that reasonable differences of opinion … are now perfectly possible. There is an acute need for simplification so that both immigrants and immigration officers may have a clearer understanding of their responsibilities and rights. (emphasis added)

Another member of the judiciary has commented, in R (on application of Iqbal) v. The Secretary of State for the Home Department [2015] EWCA Civ 838:

I cannot, however, leave this judgment without observing how abstruse the law has become in this area. That is always a weakness but particularly when so many immigrants are litigants in person with precious little, if any, understanding of English law. It is telling that in this case the Secretary of State had changed her view as to the proper interpretation of section 3c, an important provision which affects the legal rights of immigrants in numerous ways. Also it is difficult to identify precisely which laws were in force at any particular time …. The overriding impression is that the rules are changed in a piecemeal way to deal with particular problems when they arise. But firefighting is not the way to produce a rational or consistent set of rules; and the process does not sit easily with the rule of law, and in particular the principle that litigants should be able to discover the laws applicable to their circumstances. (emphasis added)

Nor is the exemption tailored to apply to a specific category of persons. Immigration offences can be committed by both British citizens (e.g., for assisting irregular entry, employing migrants without a work permit, etc.) as well as non-citizens.[[14]](#footnote-14) Moreover, as immigration status is a requirement for accessing a number of services, the government could make it mandatory to screen all users of these services to determine their eligibility. Such a scheme is not implausible, given the existence of multiple data sharing arrangements between the Home Office and various other government services:

* Home Office, the Department of Health and Social Care and National Health Service (NHS) Digital with respect to patient records (withdrawn November 2018);
* Home Office and the Department of Education with respect to children’s school records;
* Home Office and Cifas (anti-fraud agency) with respect to bank accounts;
* Home Office and Driver and Vehicle Licensing Agency with respect to driving licenses;
* Home Office, the Department for Work and Pensions, with respect to employment records and welfare benefits, including child maintenance.[[15]](#footnote-15)

Nor is the exemption limited to the Home Office or other public authorities. It applies to any entity from whom the Home Office obtains data for immigration control purposes, which could include data brokers, corporate entities, service providers, and non-governmental organizations.

The sweeping application of the exemption is particularly alarming because, in many circumstances, individuals will not know that their rights have been limited under the exemption. Because they are unaware that their personal data has been processed under the exemption, it will be impossible for them to challenge the processing of their data, to the Information Commissioner’s Office. The absence of notice also means that data subjects will have extremely limited opportunity to correct errors in that data and how it is processed. This is against the backdrop of a history of missteps by the Home Office, based on errors:

* Several cases have been reported in the press of people being deported because of errors in their immigration files.[[16]](#footnote-16)
* It has been reported that up to ten percent of sampled refusals of bank accounts to individuals on immigration grounds were made in error, due to poor data quality.[[17]](#footnote-17)

The vagueness of the “immigration control exemption”, and the breadth of its scope, make it impossible for data subjects to foresee its application; this is only reinforced by the secrecy made possible by the exemption in the processing of individuals’ personal data.

#### Derogations from data subject rights under the “immigration control exemption” are neither necessary nor proportionate

While sector-specific exceptions may be permissible under Article 23 of the GDPR (for instance, in the context of intelligence services), blanket exceptions, such as the one created under Schedule 2, Part 1, paragraph 4 of the DPA generally are not, given that their sweeping nature makes it highly likely they lack (i) proportionality and necessity, (ii) specificity in their application, and (iii) safeguards against abuses of the personal data processed under the exceptions. Such is the case here.

**The restrictions on data subject rights are not necessary**

The jurisprudence of the Court of Justice of the European Union applies a strict necessity test[[18]](#footnote-18) for any limitations on the rights to personal data protection and respect for family life in the context of processing personal data. This strict necessity applies equally to law enforcement as to commercial or other areas, because of the importance that personal data has for a range of fundamental rights. Consequently, "*derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary*".[[19]](#footnote-19)

Each aspect of the measure is subject to the strict necessity test.[[20]](#footnote-20) This assessment depends on “*clear and precise rules governing [a measure’s] scope and application”*. Clear and precise rules are important also to comply with most of the other criteria of Article 52(1) CFR.[[21]](#footnote-21) Such rules and guidance on the application of the “immigration exemption” are notably absent from the DPA.

Necessity also entails that the measure detail why existing, or less intrusive, alternatives are insufficient to address the problem; and why the proposed measure can address the problem more effectively. Significantly, the DPA does not specify how restricting data subjects’ right to information about their personal data would achieve effective immigration control, and it does not appear to rely on any research or other information to underpin its reasoning.

The UK government has justified the exemption by claiming that it is needed to forestall possible absconding by people informed of any processing of their personal data with a view to their removal, for instance, or for investigating the veracity of information provided to support an application for leave to remain in the UK.[[22]](#footnote-22) And yet no evidence has been presented to show that provisions elsewhere in the DPA (for instance, those concerning law enforcement, under Part 1 of the DPA) are inadequate to address the aims of immigration enforcement. More concerning, no evidence has been adduced about the number of people who purportedly abscond under the current legal framework, when they are provided information about processing of their data or responses to requests for information about their data. And indeed, the government has, to our knowledge, provided no evidence to support the need, or the effectiveness, of the exemption, which did not exist in the DPA’s predecessor. On 13 November 2017, Lord Clement Jones expressed the following concerns at a debate of the House of Lords Data Protection Bill Committee:

*The immigration exemption is new in the Bill; there was no direct equivalent under the Data Protection Act 1998. This is the broad and wide-ranging exemption that is open to abuse. The exemption should be removed altogether, as there are other exemptions in the Bill that the immigration authorities can, and should, seek to rely on for the processing of personal data in accordance with their statutory duties and functions. The current provision, under the heading “Immigration,” removes all rights from a data subject that the Home Office wishes it did not have. Such removals are not restricted to those who have been found guilty of immigration offences, but apply to every data subject, including Home Office clerical errors. It is exactly those errors that data protection regulates …*

*[…] The immigration authorities should be able to justify the inclusion of this exemption on the basis of hard evidence. The Home Office should be able to provide examples of subject access requests where personal data were released to the detriment of the public interest. […][[23]](#footnote-23)* (emphasis added)

Despite these concerns, the immigration exemption was retained in the final bill, passed in May 2018 without any apparent balancing of the deprivation of fundamental data protection rights of data subjects against the urgency of tackling the risk of absconding is purportedly addressed, or the measure’s effectiveness in this regard.

**The restrictions on data subject rights are not proportionate**

Broadly speaking, proportionality captures both the necessity and the appropriateness of a measure – that is, the extent to which there is a rational connection between the measure and the (legitimate) objective pursued. For a measure to meet the standard of proportionality, as established under Article 52(1) of the Charter, the advantages it generates should not be outweighed by the disadvantages it causes to the exercise of the fundamental rights.[[24]](#footnote-24)

According to the CJEU, a proportional measure is *“appropriate”* for its objective and does not *“go beyond what is necessary.”* Like the assessment of necessity, this a very factual test. In this sense, proportionality is not unrelated to the data processing principle established in Article 5(1)(c) GDPR, “data minimization”, which requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This is a crystallization of the underlying principle of data protection that “*personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*” (Recital 39 GDPR) and the proportionality principle of general EU law.

Among the broad range of factors it has considered in assessing proportionality,[[25]](#footnote-25) the European Court of Human Rights has examined whether the scope of the measure is limited, and whether safeguards are in place.

With respect to scope, we have already noted the extraordinary breadth and vagueness of the immigration exemption. The UK’s expected departure from the European Union further expands the number of people who will be affected by this exemption.

On 23 August 2018, judicial review of the DPA was sought before the High Court of Justice, on the grounds that the “immigration enforcement exemption” is a foundation of the right to privacy, as guaranteed under Articles 7 and 8 of the ECHR, and the Charter. Among other things, the complainants argue that “exemption could affect the living status of millions of people, and the rights of even more.”

*It will affect vulnerable individuals and all others that need to navigate the complicated immigration control system. There are also the 3 million European Union citizens that will be applying for settled status in the coming year.[[26]](#footnote-26)*

The complaint raises concerns about the scale of errors and delays in the immigration system, which include mistakes by immigration authorities concerning the data of third country nationals, as well EU nationals. Some of these errors resulted in some people being wrongly identified as in the UK without leave and included on the list of “disqualified persons” who received letters stating they are liable to removal and must immediately arrange their departure from the country.[[27]](#footnote-27)

With Brexit approaching, EU nationals must obtain a new “settled” status, which requires engaging with immigration authorities and other data controllers through an as-yet unspecified immigration procedure. There are significant concerns that EU nationals will join third country nationals on the lower rung of a two-tiered system whereby non-UK citizens are denied their fundamental data protection rights, with the risk of possible deportation, due to errors committed by immigration authorities charged with processing millions of applications by people at risk of losing their status due to Brexit.

There are also significant concerns about the lack of safeguards in the DPA about the exemption, including the absence of any guidelines defining how the measure will be implemented. These concerns are well summarised by the intervention of MP Yvette Cooper in the House of Commons:

*This exemption allows the Home Office to refuse subject access requests in immigration cases and to put in place data sharing without proper accountability in any case where it meets the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective control, and yet, repeatedly, we have had no explanation from Ministers as to what effective immigration control means. That is because, in truth, it is immensely broad. It could mean meeting the net migration target, sustaining the hostile environment and enabling a deportation that the Home Office thinks is justified, even if in practice it has made a mistake. It could mean decisions being taken by immigration removal centres, G4S, Serco or any of the many private companies contracted by the Home Office to deliver its so-called immigration control.*

*The Home Office has made an objective of reducing the number of appeals and removing the right to appeal in immigration cases. If a subject access request makes an appeal more likely, why does preventing that [subject access request] in order to prevent a potential appeal not count as immigration control under the Home Office’s definition? […]*[[28]](#footnote-28)

Although derogations under the “immigration exemption” are limited to data subject rights, they nonetheless represent an unjustifiable breach of fundamental data protection rights, with sweeping and potentially profound implications for a broad range and number of data subject. In spite of repeated concerns raised about its legality and likely harmful effects, this measure was adopted with on the basis of a feeble justification, but with no effort to demonstrate with evidence that it is necessary and proportionate, as required in a democratic society.

#### In the context of the UK’s current “hostile environment”, the “immigration control exemption” risks supporting further violations of the fundamental rights and freedoms of affected individuals

Article 23 GDPR requires that deviations from the GDPR’s rules “*respect[] the essence of fundamental rights and freedoms*”.

Under the “immigration control exemption”, derogation from Article 5 GDPR is only with respect to data subject rights and *does not* extend, for instance, to the repurposing of personal data for immigration control purposes. Existing measures adopted within the framework of the UK’s “hostile environment” do, however, engage in such repurposing of personal data. The “immigration control exemption” risks reinforcing such measures, by promoting their secrecy and making it harder to challenge the legality of efforts to process personal data for immigration purposes, by public and private actors. This has significant implications for the fundamental rights of affected individuals, including the rights to education, health care, housing, access to the justice system and to an effective remedy, and to non-discrimination.[[29]](#footnote-29)

##### The “hostile environment”

In 2010, the UK adopted a policy aimed at creating a “hostile environment” for people without indefinite leave to remain in the country. This policy has manifested itself in successive amendments to the Immigration Act, which, among other things, created sanctions for landlords who rent to undocumented persons, restricted the ability of people who are undocumented to obtain driver licenses and bank accounts, and introduced charging for secondary health care for people who are not “ordinarily resident” in the UK.[[30]](#footnote-30) The following examples are illustrative of the policy, and its impact:

* The Department of Education has an agreement to share data from the National Pupil Database, collected through the School Census, with the Home Office for immigration enforcement purpose, sharing the personal information of up to 1500 children each month who are believed to be undocumented.[[31]](#footnote-31)
* Over half of police forces have reported sharing data about victims of crime with the Home Office.[[32]](#footnote-32) In December 2018, the UK National Police Chiefs Council adopted new guidance on the sharing of personal data with immigration enforcement authorities asserting that someone who reports a crime to the police “*will always, first and foremost*” be “*treat[ed] as a victim*”, and that police will not check a database only to establish a victim’s immigration status. However, under this policy officers who become of aware of irregular status will not take any action themselves but are still permitted to inform immigration enforcement authorities of the victim’s irregular status.[[33]](#footnote-33)
* The Home Office, Department of Health and Social Care, and NHS Digital had an agreement allowing the Home Office to use confidential patient records to obtain the addresses of patients suspected of being undocumented. This agreement was suspended on May 2018.[[34]](#footnote-34) Between January and November 2016, NHS Digital provided the Home Office with the personal data of 5 854 patients.[[35]](#footnote-35)

Civil society actors,[[36]](#footnote-36) governmental agencies,[[37]](#footnote-37) as well as members of parliament[[38]](#footnote-38) have repeatedly raised alarms about the effects of these policies. A June 2018 parliamentary briefing on the impact of the “hostile environment” policy notes:

*The Government has stated the policies are needed to deter illegal [sic] immigration. However, the Opposition has called for an end to the policy, believing it has had a negative impact on individuals’ lives, including those with a right to live in the UK. For example, there have been a number of reports of Commonwealth migrants who have lived in the UK since before 1973 (often referred to as the ‘Windrush generation’), who have a legal right to live in the country under the Immigration Act 1971, being denied access to services and being sent letters threatening them with deportation or detention due to their inability to provide documentation of their right to reside in the UK. The Home Office has confirmed that it has identified 63 individuals who may have been wrongfully deported. In addition, the Independent Chief Inspector of Borders and Immigration has stated that there are issues monitoring the overall impact of the policy, and has highlighted occasions of people being wrongly denied access to driving licences and bank accounts or being discriminated against by landlords. Further, some commentators, such as the UN Special Rapporteur on Racism, have claimed the policy measures can cause racism and discrimination. The Government has recently legislated for and introduced a ‘Windrush scheme’ aimed at rectifying some of the issues suffered by the ‘Windrush generation’ individuals. In addition, the Home Secretary, Sajid Javid, stated on 3 June 2018 that many of the ‘compliant environment’ policy measures were now being reviewed.[[39]](#footnote-39)*

The “hostile environment” policy includes as one of its key elements the ‘Right to Rent’ scheme, which was introduced in 2016 as a part of the Immigration Act.[[40]](#footnote-40) The scheme aims to ensure that only people with a right to remain in the UK can access the private rental market. To prevent rentals to undocumented tenants, the scheme obliges landlords to check the immigration status of tenants and potential tenants. Renting property to undocumented people puts landlords at risk of fines or imprisonment up to five years. In result, the policy delegates immigration control duties to third parties, and there have been longstanding concerns that it results in discrimination against ethnic minority groups.

Despite the fact that the policy is aimed at non-EU nationals without a valid permit to stay in the UK, there are reports that people with a right to be present in the country (including UK nationals, EU nationals, and non-EU nationals holding a valid leave) have been affected by the policy due to errors in applications process or problems with data retained by the Home Office. The Joint Council for the Welfare of Immigrants challenged the scheme and on March 1, 2019 the High Court of Justice ruled that the scheme is incompatible with human rights, having caused indirect racial discrimination in a manner that deprived people of their right to have a family and private life. In consequence, the law must be amended so that it is compatible with the Article 8 (family and private life) and Article 14 (prohibition of discrimination) of the ECHR.[[41]](#footnote-41)

There is therefore a solid foundation of evidence concerning the harmful impact of existing policies that deviate from the rights established under the GDPR, aimed at repurposing personal data obtained in one setting (e.g., provision of health care) for immigration control. This is the policy environment in which the DPA’s “immigration exemption” was enacted. The restrictions it creates in connection with data subject rights must be understood within this context, and in terms of how they generate new layers of secrecy that shield various governmental and private actors from accountability for the improper processing of personal data.

Article 21(1) of the Charter establishes that discrimination based on any ground shall be prohibited. It is already the case that existing measures arising from the “hostile environment” policy have had a disproportionate impact on minority communities, and individuals in situations of vulnerability. The “immigration control exemption” furthers violations of rights of non-citizens, including the rights to education, health care, housing, access to the justice system and to an effective remedy, and to non-discrimination.[[42]](#footnote-42)

#### The “immigration control exemption” fails to establish the safeguards required under Article 23(2) GDPR

Even if the exemption could be said to meet the strict conditions set out in Article 23(1), it fails to include procedural safeguards set out in 23(2) that require that any measure taken under Article 23(1) contain specific provisions to prevent abuse or unlawful access or transfer of personal data, including through the specification of the controller or categories of controllers, storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing, and the risks to the rights and freedoms of affected individuals.

The absence of such safeguards is particularly problematic in view of the GDPR’s enhanced protections for sensitive data, and for vulnerable data subjects.

##### Sensitive data

GDPR enforces enhanced protection for certain special categories of data (“sensitive data”). The processing of sensitive data is in principle prohibited by GDPR, unless certain exceptions apply.[[43]](#footnote-43) The enhanced protection of sensitive data is inherently linked to (and must therefore be read in light of) other fundamental rights, such as the freedom of thought, conscience and religion protected by Article 9 ECHR and the prohibition of discrimination protected by Article 14 ECHR.

Information concerning a person’s immigration status will often indirectly qualify as sensitive data because it may reveal the individual’s racial or ethnic origin and, particularly in the case of asylum seekers or refugees, political opinions, religious or philosophical beliefs and/or sexual orientation.

##### Vulnerable Data Subjects (Children)

Specific categories of individuals that are particularly vulnerable are also entitled to a higher level of protection under GDPR, including children.[[44]](#footnote-44)  Children should enjoy stronger protection when their personal data are used for any purpose, including to check their immigration status.[[45]](#footnote-45) The “immigration control exemption” is bereft of limitations that safeguard the special rights of vulnerable individuals, and in particular children.

#### Conclusion

The UK DPA’s “immigration control exemption” runs exactly contrary to the EU’s efforts to reinforce individuals’ fundamental right to the protection of their personal data through the GDPR, particularly in the age of Big Data. It carves out a space where public and private actors have wide discretion to process personal data, without the knowledge of affected individuals and thus with virtually no accountability, for the broad and unspecified aim of “immigration enforcement.” Such an exemption flies in the face of the EU’s standards on privacy and data protection, as well as rights to due process and to an effective remedy. It does not meet the strict conditions set out in Article 23 for derogations of rights under the GDPR.

For the reasons outlined above, the UK DPA’s “immigration control exemption” is wholly incompatible with the GDPR and risks the future adequacy of the UK’s data protection arrangements for the free flow of data between the UK and the EU. The exemption is also incompatible with Articles 8 and 14 of the European Convention on Human Rights, and Articles 7, 8, 20, 21, 24 and 47 of the EU Charter of Fundamental Rights.

1. The name of the EU country and national, regional, or local authority or authorities that you believe have breached Union law:

United Kingdom

1. Union laws (e.g. Treaties, regulations, directives, decisions and case law) or principles underpinning Union law that you believe to have been breached by the authorities of the EU country concerned:

* *Treaty on the Functioning of the European Union*
* *EU Charter of Fundamental Rights*
* *European General Data Protection Regulation*

1. The specific national measures (national law or other regulatory or administrative measures) that you believe to infringe Union law, and why these breach Union law:

* *UK Data Protection Act 2018*

1. Does the EU country concerned receive EU funding relating to the issue that prompted your complaint, or may it receive such funding in future?

None identified

1. What specific action are you requesting the European Commission should take?

We respectfully call upon the European Commission to launch an urgent investigation into this matter and to take appropriate measures to ensure respect by the United Kingdom of its Treaty obligations.

We also request the European Commission apply for interim measures before the Court of Justice of the European Union in accordance with Article 279 TFEU and Article 29 of Protocol (No 3) on the Statute of the Court of Justice of the European Union, with a view to obtaining an order directed to the United Kingdom ordering it to suspend the operation of the UK rules on data protection while the Commission’s investigation in pending.

We further request that the European Commission take due account of the above in its assessment of the future adequacy of the UK’s data protection arrangements for the free flow of data between the UK and the EU.

## Does your complaint relate to the EU Charter of Fundamental Rights, which applies only to the implementation of Union law (Article 51)?

*Article 7 (respect for private and family life)*

*Article 8 (protection of personal data)*

*Article 20 (equality before the law)*

*Article 21 (non-discrimination)*

*Article 24 (rights of the child)*

*Article 47 (right to an effective remedy and to fair trial)*

## If possible, please provide a list of documents or evidence in support of your complaint (including the national measures concerned) that you can send to the Commission if it so requests:

* *A Guide to Hostile Environment. The border controls dividing our communities – and how can we bring them down*, Edited by LIBERTY, April 2018, available at < <https://www.libertyhumanrights.org.uk/sites/default/files/HE%20web.pdf>>.
* *“No Passport Equals No Home”: An independent evaluation of the ‘Right to Rent’ scheme*, Joint Council for Welfare of Immigrants, September 2015, available at < <https://www.jcwi.org.uk/Handlers/Download.ashx?IDMF=5ab15f33-ae32-4e66-b040-402b71392177>>.
* *The hostile environment for immigrants How Theresa May has created an underclass in the UK*, Global Justice Now, February 2018, available at < <https://www.globaljustice.org.uk/sites/default/files/files/resources/hostile_environment_briefing_feb_2018_web.pdf>>.
* Judgement from 1 March 2019 of England and Wales High Court (Administrative Court) Decisions, before: MR JUSTICE MARTIN PENCER, between: R (Joint Council for the Welfare of Immigrants) and Secretary of State for the Home Department, available at < <https://www.bailii.org/ew/cases/EWHC/Admin/2019/452.html>>.
* House of Commons Home Affairs Committee Immigration policy: basis for building consensus Second Report of Session 2017–19, available at <<https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/500/500.pdf>>.
* *The Right to Rent Scheme and the Impact on the Private Rented Sector*, Noora Mykkanen, Dr Tom Simcock, Residential Landlords Association, December 2018, available at <<https://research.rla.org.uk/wp-content/uploads/right-to-rent-impact-private-renting-2018.pdf>>
* *Care don’t share,* Liberty, December 2018, available at <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%20%27Care%20Don%27t%20Share%27%20Report%20280119%20RGB.pdf>>.
* Migrants’ Rights Network (Claimant) and The Secretary of State for the Home Department and The Secretary of State for Health (Defendants), Statement of Facts and Grounds, The High Court of Justice, Queen’s Bench Division, Administrative Court.

# APPEALS / LEGAL ACTIONS / OTHER ACTIONS

**7. Have you already taken action in the EU country concerned to attempt to solve this problem, or are you aware of any action in the country concerned covering the issue you raise in this complaint?**

Yes (X) No ( )

**8. If you answered yes to point 7, what action have you already taken in the country concerned to tackle the problem?**

*( ) Administrative action (e.g. appeals; complaints to the relevant public authorities; complaint to a national regional ombudsman)*

*If applicable, please state what type of decision(s) resulted from the administrative procedure.*

*Where applicable, please provide a list of your correspondence/contacts with public authorities. Include a short summary of the correspondence.*

*(X) Legal action (recourse to courts)*

*Please state whether your action has been settled by a court or is pending before a court. If the case is pending, when can a decision be expected?*

PICUM is aware of one legal action challenging the “immigration control exemption” of the DPA, by The Open Rights Group and the3million (Claimants) against the Secretary of State for the home Department, the Secretary of State for Digital, Culture, Media and Sport.

Statement of Facts and grounds were filed on 23 August 2018 with the High Court of Justice, Queen’s Bench Division, Administrative Court; and a hearing of the merits is scheduled for July 2019.

**9. If you answered no to point 7, please consider taking action in the EU country concerned to tackle your problem. You will be able to assert your rights directly and personally by using national means of redress.**

**If you have decided not to take action to tackle your problem in the country concerned, why not?**

( ) No remedy available for the problem

( ) The remedy exists, but it is too costly

( ) Time limit for action has expired

( ) No legal standing (indicate why you are not eligible for this particular remedy)

( ) No legal aid / no lawyer

( ) I do not know what remedies are available for the problem

( ) Other (please specify)

**10. Please indicate whether you have already contacted other EU institutions and bodies to request help in solving your problem:**

( ) European Parliament – Petitions

( ) European Ombudsman

( ) Other (please specify)

*Please give the reference assigned to your complaint, file, correspondence, etc. by the institution or body concerned.*

**11. If, after examining your case, the Commission considers that SOLVIT is better placed to deal with it, do you agree to your complaint being transferred to SOLVIT?**

( ) Yes, I agree that the Commission can transfer my complaint to SOLVIT.

(X) No, I do not agree to the Commission transferring my complaint to SOLVIT.

**12. Specify any documents or evidence which may be submitted in support of the complaint, including the national measures concerned (attach copies):**

See response to section 6, above.

**IV. CONFIDENTIALITY – DATA PROTECTION**

(X) I authorise the Commission to disclose my identity in its contacts with the authorities of the EU country against which I am lodging a complaint.

( ) I do not authorise the Commission to disclose my identity in its contacts with the authorities of the EU country against which I am lodging a complaint.

**Place, date and signature of complainant/representative:**

1. European Convention for the Protection of Human Rights and Fundamental Freedoms. [↑](#footnote-ref-1)
2. Convention 108 for the Protection of Individuals with regard to automatic processing of personal

   data. [↑](#footnote-ref-2)
3. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in

   2013. [↑](#footnote-ref-3)
4. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European

   Community, signed at Lisbon, 13 December 2007. [↑](#footnote-ref-4)
5. CJEU, Case C-553/07 (*Rijkeboer*), judgment of May 7, 2009, § 47; CJEU, Joined Cases C-293/12 and

   C-594/12 (*Digital Rights Ireland and Others*), judgment of April 8, 2014, § 53; CJEU, Case C-131/12

   (*Google Spain and Google*), judgment of May 13, 2014, §§ 53, 66 and 74. [↑](#footnote-ref-5)
6. See, for example, CJEU, Case C-362/14 (*Schrems*) judgment of October 6, 2015, § 38: “[T]he

   provisions of [DPD], inasmuch as they govern the processing of personal data liable to infringe

   fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in

   the light of the fundamental rights guaranteed by the Charter.” [↑](#footnote-ref-6)
7. Recital 73 of GDPR; Article 29 Working Party, WP 211, Opinion 01/2014 on the application of

   necessity and proportionality concepts and data protection within the law enforcement sector, adopted on

   February 27, 2014; on safeguarding irregularly present migrants from discrimination in a human rights

   context, see also ECRI General Policy Recommendation No. 16 on safeguarding irregularly present

   migrants from discrimination, adopted on March 16, 2016. [↑](#footnote-ref-7)
8. For example, Case CJEU, F-46/09 (*EU Civil Service Tribunal*), judgment of July 5, 2011, §§ 122-127

   (on medical data). [↑](#footnote-ref-8)
9. See, specifically with respect to deviations from the purpose limitation principle discussed below,

   Article 29 Working Party, WP 203, Opinion 03/2013 on purpose limitation, adopted on April 2, 2013, p.

   37-38. [↑](#footnote-ref-9)
10. Recital 19, [Amendments by the European Parliament to the Commission Proposal](http://www.europarl.europa.eu/sides/getDoc.do?type=AMD&format=PDF&reference=A8-0201/2018&secondRef=047-047&language=EN), 24.9.2018, A8-0201/2018. [↑](#footnote-ref-10)
11. For example, Case CJEU, F-46/09 (*EU Civil Service Tribunal*), judgment of July 5, 2011, §§ 122-127 (on medical data). [↑](#footnote-ref-11)
12. CJEU, Case C-465/00 (*Rechnungshof*), Judgment of May 20, 2003, § 82-90, 94. [↑](#footnote-ref-12)
13. See one practitioner’s comments at Colin Yeo, 24 January 2018, “[How complex is UK immigration](https://www.freemovement.org.uk/how-complex-are-the-uk-immigration-rules-and-is-this-a-problem/)

    [law and is this a problem?](https://www.freemovement.org.uk/how-complex-are-the-uk-immigration-rules-and-is-this-a-problem/)” [↑](#footnote-ref-13)
14. Migration Observatory. [↑](#footnote-ref-14)
15. *See* Liberty (2018), [Care Don’t Share - Hostile Environment Data-Sharing: Why We Need A Firewall](https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%20%27Care%20Don%27t%20Share%27%20Report%20280119%20RGB.pdf)

    [Between Essential Public Services and Immigration Enforcement](https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%20%27Care%20Don%27t%20Share%27%20Report%20280119%20RGB.pdf). [↑](#footnote-ref-15)
16. ‘Leave the UK immediately’: scientist is the latest victim of Home Office blunder,’ *The Guardian*, 26

    September 2017. [↑](#footnote-ref-16)
17. An inspection of the ‘hostile environment’ measures relating to driving licenses and bank accounts, October 2016, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567652/ICIBI-hostile-environmentdriving-licences-and-bank-accounts-January-to-July-2016.pdf> [↑](#footnote-ref-17)
18. See e.g., C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238C-698/15 *Tele2 Sverige AB v Post-ochtelestyrelsen and Secretary of State for the Home Department v Tom Watson and others* [2016] ECLI:EU:C:2016:970; Case C-362/14 *Maximilian Schrems v.Data Protection Commissioner* [2015] ECLI:EU:C:2015:650. [↑](#footnote-ref-18)
19. See European Data Protection Supervisor (11 April 2017), [Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf). It is also relevant to consider the ECtHR’s test for necessity – that is a measure “*necessary in a democratic society*” – which, in the context of the protection of personal data, means that it must address “*a pressing social need”*. See e.g., *S and Marper v United Kingdom* Apps nos 30562/04 and 30566/04 (ECHR, 4 December 2008), para 101. [↑](#footnote-ref-19)
20. Id. [↑](#footnote-ref-20)
21. *Dudgeon v United Kingdom* Appl. No. 7525/76 (ECtHR 22 October 1981) Par 60. [↑](#footnote-ref-21)
22. Baroness Williams of Trafford, Minister of State, Home Department, Debate in House of Lords on Data Protection Bill, 13 November 2017, available at <https://www.theyworkforyou.com/lords/?id=2017-11-13b.1898.0>. [↑](#footnote-ref-22)
23. Lord Clement-Jones, Artificial Intelligence Committee, Liberal Democrat Lords Spokesperson (Digital), Part of Debate in House of Lords on Data Protection Bill, 13 November 2017, available at <https://www.theyworkforyou.com/lords/?id=2017-11-13b.1908.3>. [↑](#footnote-ref-23)
24. See European Data Protection Supervisor (11 April 2017), [Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf) (“EDPS Toolkit”). [↑](#footnote-ref-24)
25. EDPS [Toolkit](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf). [↑](#footnote-ref-25)
26. First Witness Statement of Matthew Rice, Open Rights Groups and the3Million v. The Secretary of State for the Home Department and the Secretary of State for Digital, Culture, Media, and Sport, 23 August 2018, at para. 8. [↑](#footnote-ref-26)
27. <https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/500/500.pdf>>. [↑](#footnote-ref-27)
28. Yvette Cooper, Chair, Home Affairs Committee, Part of Data Protection Bill, House of Commons, 9 May 2018, available at <https://www.theyworkforyou.com/debates/?id=2018-05-09a.771.1>. [↑](#footnote-ref-28)
29. UN Committee on Economic, Social and Cultural Rights (13 March 2013) E/C.12/2017/1, [Duties of States towards refugees and migrants under the International Covenant on Economic, Social and Cultural Rights – Statement by the Committee on Economic, Social and Cultural Rights](http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=4slQ6QSmlBEDzFEovLCuW1AVC1NkPsgUedPlF1vfPMJbFePxX56jVyNBwivepPdlEe4%2BUb4qsdJhuBDpCRSOwCXPjZ7VN7SXN0oRoXkZhCuB9Z73iyU35LZveUjX0d7u). [↑](#footnote-ref-29)
30. “Ordinarily resident” is defined as non-EEA citizens with indefinite leave to remain. Other longer-term visa holders are required to pay an immigration health surcharge to access all NHS services; overseas visitors are charged 150% of the normal tariff and Clinical Commissioning Groups and hospitals have a duty to report to the Home Office any patients who owe ₤500 or more for two months, who have no negotiated payment plan. Holders of visitors’ visas and undocumented migrants are the main chargeable groups under current rules. [↑](#footnote-ref-30)
31. Damien Gayle, 15 December 2016, “[Pupil data shared with Home Office to ‘create hostile environment’ for illegal migrants](https://www.theguardian.com/uk-news/2016/dec/15/pupil-data-shared-with-home-office-to-identify-illegal-migrants)”, *The Guardian.* [↑](#footnote-ref-31)
32. Catrin Nye, Natalie Bloomer and Samir Jeraj, 14 May 2018, “[Victims of serious crime face arrest over immigration status](https://www.bbc.co.uk/news/uk-44074572)”, *BBC*. See also Samir Jeraj, Natalie Bloomer, 28 November 2017, “[Woman reports rape to police – and is arrested on immigration charges](http://www.politics.co.uk/news/2017/11/28/woman-reports-rape-to-police-and-is-arrested-on-immigration),” *Politics.* [↑](#footnote-ref-32)
33. NPCC Press Release, 7 December, “[New guidance for officers on sharing information with Immigration Enforcement](https://news.npcc.police.uk/releases/new-guidance-for-officers-on-sharing-information-with-immigration-enforcement).” [↑](#footnote-ref-33)
34. Denis Campbell, “[NHS will no longer have to share immigrants’ data with Home Office](https://www.theguardian.com/society/2018/may/09/government-to-stop-forcing-nhs-to-share-patients-data-with-home-office),” *The Guardian,* 9 May 2018. [↑](#footnote-ref-34)
35. Alan Travis, 24 January 2017, “[NHS hands over patient records to Home Office for immigration crackdown](https://www.theguardian.com/uk-news/2017/jan/24/nhs-hands-over-patient-records-to-home-office-for-immigration-crackdown)”, *The Guardian.*  [↑](#footnote-ref-35)
36. See, e.g., Liberty, A Guide to the Hostile Environment, April 2018. [↑](#footnote-ref-36)
37. Independent Chief Inspector of Borders and Immigration, *An Inspection of the ‘Right to Rent’ Scheme*, March 2018. [↑](#footnote-ref-37)
38. See, e.g., UK Parliament, “Memorandum of understanding on data-sharing inquiry”, <https://www.parliament.uk/business/committees/committees-a-z/commons-select/health-committee/inquiries/parliament-2017/mou-data-sharing-nhs-digital-home-office-inquiry-17-19/>. [↑](#footnote-ref-38)
39. Russell Taylor, “Impact of the ‘hostile environment’ policy debate on 14 June 2018”, *House of Commons*, 11 June 2018. [↑](#footnote-ref-39)
40. Immigration Act 2016, Part 2 Access to Services, Residential tenancies, Section 33A. available at <http://www.legislation.gov.uk/ukpga/2016/19/part/2/enacted>. [↑](#footnote-ref-40)
41. JCWI v. Secretary of State for the Home Department [2019] EWHC 452 (Admin) (1 March 2019), available at <https://www.bailii.org/ew/cases/EWHC/Admin/2019/452.html>. [↑](#footnote-ref-41)
42. In March 2016, the European Commission against Racism and Intolerance (ECRI) published General Policy Recommendation No. 16 (GPR 16) on safeguarding irregularly present migrants from discrimination. GPR 16 addresses “*the pressing issue of discrimination which is causing grievous hardship to a substantial number of migrants who are irregularly present in member states*,*”* presenting recommendations on how to safeguard their rights under international human rights instruments, particularly in the areas of education, health care, housing, social security and assistance, labour protection and justice. ECRI’s central recommendation to states is the creation of “*firewalls*” that “*prohibit the sharing of personal data*”about people in an irregular situation “*with the immigration authorities for purposes of immigration control and enforcement.*” ECRI (2016), [Safeguarding irregularly present migrants from discrimination](https://reliefweb.int/sites/reliefweb.int/files/resources/REC-16-2016-016-ENG.pdf). See also Francois Crepeau, Bethany Hastie, *European Journal of Migration and Law*, “The Case for ‘Firewall’ Protections for Irregular Migrants: Safeguarding Fundamental Rights,” 157-183 (17 May 2016). [↑](#footnote-ref-42)
43. Article 9(1) of GDPR; Recital 51 of GDPR recognizes that the processing of these types of data “*could*

    *create significant risks to the fundamental rights and freedoms*”, of individuals. [↑](#footnote-ref-43)
44. Recital 75 of GDPR; the term “*child*”is not defined by GDPR and one must assume all legal minors of

    age (as defined under national law) should be offered enhanced protection (see also Recital 38 of GDPR). [↑](#footnote-ref-44)
45. Examples where GDPR offers specific protection to children include: (i) the rights and freedoms of a

    data subject may “*in particular*”override the interests of the controller who is relying on legitimate

    interests for processing “*where the relevant data subject is a child*” (Article 6(1)(f) of GDPR); (ii) when

    processing of personal data is based on consent, parental consent must be obtained for information

    society services offered directly to a child under the age of 16 (Article 6(1)(f) of GDPR); (iii) The obligation

    on controllers to ensure that information provided to data subjects is concise, transparent and in plain

    language is to be met “*in particular for any information addressed specifically to a child*” (Recital 58 of

    GDPR). [↑](#footnote-ref-45)