SUBMISSION TO THE INFORMATION COMMISIONER

–

REQUEST FOR AN ASSESSMENT NOTICE OF POLITICAL CONSULTANCIES:

The "CT" group of companies

A. Introduction and purpose of this submission

1. This submission seeks to highlight concerns about the data processing of one particular data consultancy, so that they may be taken into account as part of the Commissioner's ongoing work relating to the use of personal data in the political process. Privacy International applauds the work the Commissioner has done in respect of highlighting the misuse of personal data in modern democratic processes, and the need to improve compliance of political operators with data protection legislation in order to rebuild and maintain trust for the system. We further welcome the continued audit of the political parties by the Commissioner.

2. As the Information Commissioner is aware, Privacy International was and remains very concerned about the practices of data brokers, like Experian and Equifax. We made a detailed submission to the Commissioner in this regard while the Commissioner was assessing the practices of those companies.[1] This current submission arises due to related concerns about the activities of political consultancies. Privacy International is concerned by the data processing activities of this industry, particularly in the context of how those processing activities impact democratic processes in the UK and beyond.[2]

[1] Privacy International, Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad, https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad
[2] Privacy International, Data and Elections, https://privacyinternational.org/learn/data-and-elections; Privacy International, Why we're concerned about profiling and micro-targeting in elections, https://privacyinternational.org/news-analysis/3735/why-were-concerned-about-profiling-and-micro-targeting-elections; Privacy International, Challenging Data Exploitation in Political Campaigning: PI Recommendations, https://privacyinternational.org/advocacy/3981/challenging-data-exploitation-political-campaigning-pi-recommendations

3. As Privacy International – unlike the Information Commissioner – does not have the power to compel an investigation into the activities of such consultancies, it bases this submission on an analysis of what information is publicly available about the practices of one such consultancy. The focus of this submission is the CT group of companies. As set out in more detail below, it is not clear which of the CT companies operating under the "CT Group" umbrella[3] are involved in the group's political consultancy offerings. However, it is known that one of the wider group of companies, CTF Partners (currently named "CT Partners"), provided consultancy services in the context of the 2019 General Election.[4] This submission sets out that analysis conducted by Privacy International (see paras 22 – 27 below), identifying, in particular, where a full assessment is needed to determine whether the processing being undertaken is lawful. The hope is that this submission will assist the Commissioner in not only assessing the practices of CT as a group of companies but will also assist with an assessment of the compliance of the political consultancy industry as a whole with data protection law. We understand that the CT Group, and/or members of it, may already be under investigation by the Information Commissioner. The *Guardian* has reported[5] on an investigation into the company CTF Partners Limited, which was the name of CT Partners Limited, a member of the CT group, before they changed name (see paragraphs 31 - 41 below).

4. Our analysis of the conduct of the CT group of companies[6] involved contrasting that conduct to their data processing Privacy Notice. We refer to the group as "CT" herein. We found a disconnect between information communicated to data subjects and the data processing that the controllers are, to the best of our knowledge, undertaking. Whilst this submission focuses on CT as a group of companies, as we stress above, we consider the problems identified about CT to be indicative of problems across the industry.

[3] Made up of CT Group Holdings Ltd, CT Group Ltd and CT Partners Ltd. See paras 31 - 41 below for further information
[4] See spending returns from the 2019 General election:
http://search.electoralcommission.org.uk/Search/Spending?currentPage=1&rows=20&sort=TotalExpenditure&order=desc&tab=1&et=pp&includeOutsideSection75=true&evt=ukparliament&ev=3696&optCols=ExpenseCategoryName&optCols=AmountInEngland&optCols=AmountInScotland&optCols=AmountInWales&optCols=AmountInNorthernIreland&optCols=DatePaid
[5] https://www.theguardian.com/politics/2019/apr/04/inquiry-launched-into-data-use-from-no-deal-brexit-ads-on-facebook
[6] https://ctgroup.com/

5. This submission is based, in particular, on information provided by CT on their website and publicly available information about CT. We have identified, in summary, having reviewed he available information, we have identified the following issues:

   i. **Data controller** – It is not clear which company or companies within the CT group is or are data controllers for the processing of the public's data in the context of election or other political campaigns, and which entities have access to personal data.

   ii. **Transparency notices** – The CT group's data processing notices[7] are defective and do not provide sufficient information for a data subject to know what data is being processed, its source and recipients or how to exercise rights over that data.

   iii. **Legal bases** – The legal bases for processing are not clear and as such, it is not clear that the data controllers have a lawful base for any or some of the data processing being undertaken. Such processing is likely to include special category data, including personal data revealing political opinions.

   iv. **Data subject rights** – The failure to be transparent with how personal data is being processed has consequent effects for the ability of data subjects to exercise their rights.

6. Thus, in the particular case of CT group, Privacy International seeks: (a) a full investigation into the activities of CT, and (b) in the light of the results of that investigation, any necessary further action by the Information Commissioner that will protect individuals from widescale and systematic infringements of the data protection legislation.

[7] https://ctgroup.com/privacy-policy/

7. As noted above, the companies within the CT group are not the only companies involved in questionable data practices in the context of election and political campaigns: the problems set out below relating to CT are illustrative of systemic issues within the political consultancy industry. This is an industry which is increasingly reliant on gathering significant amounts of personal data and exploiting that data to target their services and to make commercial profit, with scant regard to their obligations under data protection laws and the rights of data subjects. Thus, for this and the further reasons detailed in this submission, it is imperative that the Information Commissioner not only investigates this specific group of companies operating in political campaigning, but also takes action in respect of other relevant actors in these industries and / or their general business practices.

B. Privacy International

8. Privacy International is a non-profit, non-governmental organisation (Charity Number 1147471) based in London that works globally at the intersection of modern technologies and human rights. Established in 1990, Privacy International is committed to protecting people's privacy, dignity and freedoms from abuses by companies and governments. Through research, litigation and advocacy, it works to build a better future where technologies, laws, and policies contain modern safeguards to protect people and their data from exploitation. As such, Privacy International has statutory objectives which are in the public interest and is active in the field of the protection of data subjects' rights and freedoms. This submission relates to Privacy International's ongoing work on "*Defending Democracy and Dissent*"[8]. We campaign to improve regulatory safeguards against political data exploitation by advocating for enforcement of existing safeguards and the introduction or reform of others.

[8] https://privacyinternational.org/long-read/3737/defending-democracy-and-dissent-year

C. Background

9. The use of personal data during the electoral process has become of major public concern. That public concern was exemplified by the scandal surrounding Cambridge Analytica and their parent company, SCL.[9] While Cambridge Analytica caught the public attention, that company was only one of many political consultancies involved in similar practices.[10] The wider industry has not been subjected to the same level of scrutiny to date, despite the Commissioner's pioneering work in this area (including her recent action in respect of data brokers).

i. The Information Commissioner's work on political data

10. On 11 July 2018, the Commissioner released two reports: (i) *Democracy Disrupted*[11] and (ii) an update on the *Investigation into the use of data analytics in political campaigns*[12].

    i. *Democracy Disrupted* focussed on the impact that digital campaigning has had on democracy, with a particular focus on how political parties use personal data. The report highlighted the growing trend of political parties relying on third parties to conduct data analytics (including profiling) and marketing.

    ii. The update on the *Investigation into the use of data analytics in political campaigns* highlighted the dangers of such third parties using data without due regard for data protection laws. The Commissioner highlighted the conduct of SCL and Cambridge Analytica as of particular concern, outlining the enforcement steps that the Commissioner had taken against those companies. The Commissioner found that had SCL

[9] See, Hankey et al, the Constitution Society, *Data and Democracy in the Digital Age* (10 July 2018) https://consoc.org.uk/publications/data-and-democracy-in-the-digital-age/; Naik et al, Oxford University, *Political Campaigning: the law, the gaps and the way forwards* (19 October 2019) https://oxtec.oii.ox.ac.uk/publication/legal-framework/
10 Privacy International, https://privacyinternational.org/long-read/4374/data-exploitation-and-political-campaigning-company-guide-resource; Tactical Tech, The Influence Industry: The Global Business of Using Your Data in Elections https://ourdataourselves.tacticaltech.org/posts/influence-industry/
[11] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf
[12] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

not dissolved, the Commissioner's "*intention would have been to issue the company with a substantial fine for very serious breaches of principle one of the DPA1998 for unfairly processing people's personal data for political purposes…*"

11. Following that report, the Commissioner has taken further significant strides to protect personal data from misuse by political parties and during democratic processes. For instance, the Commissioner has issued draft guidance on the use of personal data for political purposes and issued a further update in respect of action taken against political parties.[13] However, political consultancies continue to process data for and on behalf of political parties with less scrutiny than that which has been afforded to date to the activities of political parties.

ii. Political consultancies

12. Whilst SCL and Cambridge Analytica have dissolved, a number of political consultancies continue to operate in the UK. Indeed, while it is not confirmed whether SCL or Cambridge Analytica ever worked directly on a British general election campaign, a number of political consultancies have operated in general elections and on behalf of major political parties.[14]

13. The work and roles of those consultancies are often opaque. They are also invisible to the wider public, despite their prominent role in electoral politics. The Commissioner highlighted the problem of transparent use of third parties in *Democracy Disrupted.*[15] In particular, the electorate often has to wait for spending returns to be released to begin to see what third parties were used by the parties during an election. This was a particular problem in respect of the 2019 General Election.

[13] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf
[14] See, for instance, *Democracy Disrupted;* Tactical Tech, The Influence Industry: The Global Business of Using Your Data in Elections https://ourdataourselves.tacticaltech.org/posts/influence-industry/; Hankey et al, the Constitution Society, *Data and Democracy in the Digital Age* (10 July 2018) https://consoc.org.uk/publications/data-and-democracy-in-the-digital-age/; Naik et al, Oxford University, *Political Campaigning: the law, the gaps and the way forwards* (19 October 2019) https://oxtec.oii.ox.ac.uk/publication/legal-framework/ etc.
[15] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

iii. 2019 election

14. A General Election was held in the UK on 12 December 2019. At the time, it was unknown whether and which third-party consultancies were used by the major political parties. We understand that members of the Open Rights Group[16] have filed a complaint with the Commissioner about that lack of transparency and other concerns about the use of data by the political parties themselves.

15. Political party spending at elections is governed by Part V of the Political Parties, Elections and Referendums Act 2000 (PPERA). Section 72(2) of PPERA defines 'campaign expenditure' as '*expenses incurred by or on behalf of a registered political party which are expenses falling within Part I of Schedule 8 and so incurred for election purposes.*' This includes, at Schedule 8 part 1 paragraph 1 (5) "*Market research or canvassing conducted for the purpose of ascertaining polling intentions*." According to the Electoral Commission's Draft Code of Practice[17] on qualifying expenses for political parties, "*market research or canvassing*" includes the use of data analytics to facilitate market research or canvassing.

16. The Electoral Commission released spending returns for the 2019 General Election on a piecemeal basis throughout 2020.[18] The Electoral Commission cited the coronavirus pandemic as the basis for the delayed release of the spending returns.

17. Of the two main political parties, the spending returns for Conservative and Unionist Party were published first. Those returns were published on or around 28 September 2020. Of those returns, Privacy International noted that CTF Partners Limited (as explained below, the company was called at the time of the 2019 Elections) was cited as the main company used by the Conservative and Unionist Party (Conservative Party) for "*Market research / canvassing services"*.

[16] https://digit.fyi/open-rights-group-attacks-uk-political-party-data-profiles/
[17] See: https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Political-parties-code-of-practice.pdf
[18] See spending returns from the 2019 General election: http://search.electoralcommission.org.uk/Search/Spending?currentPage=1&rows=20&sort=TotalExpenditure&order=desc&tab=1&et=pp&includeOutsideSection75=true&evt=ukparliament&ev=3696&optCols=ExpenseCategoryName&optCols=AmountInEngland&optCols=AmountInScotland&optCols=AmountInWales&optCols=AmountInNorthernIreland&optCols=DatePaid

From a total of £4,471,937 spent on "*Market research and canvassing services*", **£1,689,000** went to CTF Partners Limited.[19]

18. It is not clear from those spending returns what CTF Partners did for the Conservative Party, as the invoices released by the Electoral Commission contain such limited information as to be meaningless, such as "*for research*".[20] However, as "*market research/canvassing*" includes "*data analytics for the purpose of ascertaining political intentions*", CTF Partners may have engaged in such conduct. As the CT group of companies is known for their use of personal data in electoral campaigns, it would be very likely that such activities were part of CTF Partners' services. CT's website lists their services[21] as follows:

> *"Opinion research*
> *C|T Group's unique research capability gets to the heart of a matter. It is designed to provide insight that can be acted on to get the results our clients seek. We identify not just what audiences think about an issue, but also why they hold their views and what factors and messages are most persuasive in shifting opinion and behaviour.*
>
> *We offer a full range of qualitative and quantitative research methods – designed, run and analysed in-house using our uniquely trained personnel and our own dedicated field houses – yielding reliable, high-quality data. We always design, conduct and analyse research projects in close collaboration with our clients in order to provide them with actionable insight, not just commentary.*
>
> *We regularly conduct community, customer and stakeholder surveys, as well as in-depth interviews and focus groups. Depending on the requirements, we can do these both in person, or remotely online. Using experienced and highly trained researchers, we are able to generate insight*

[19] See spending returns from the 2019 General election: http://search.electoralcommission.org.uk/Search/Spending?currentPage=1&rows=20&sort=TotalExpenditure&order=desc&tab=1&et=pp&includeOutsideSection75=true&evt=ukparliament&ev=3696&optCols=ExpenseCategoryName&optCols=AmountInEngland&optCols=AmountInScotland&optCols=AmountInWales&optCols=AmountInNorthernIreland&optCols=DatePaid
[20] For example, http://search.electoralcommission.org.uk/English/Spending/SP0508444
[21] https://ctgroup.com/expertise/

that provides our clients with an evidence-base and strategy for action. We help businesses better engage their employees, communicate more effectively with communities and identify emerging consumer preferences.

Data analytics

Our ability extends to providing all fieldwork options, easy-to-use data table outputs, and full service analysis and reporting to give our clients actionable insight. Our insights assist clients with the strategic development of their brand, product and service.

Multi-channel and multi-market evaluation research

Utilising our research expertise we are regularly asked to evaluate the performance of campaigns. We can do this across multiple channels and markets, helping businesses understand not only whether their message is reaching the right audience, but also that it is having the desired results. We do this via a unique combination of survey and digital listening tools, delivering live and rolling information on the effectiveness of the campaign across different channels, so budgets can be allocated more effectively and precisely to drive impact.

Behaviour change research

Building on decades of experience helping to identify voting behaviours during election campaigns, the C|T Group can apply learned techniques and technical knowhow to help organisations overcome what can often be significant and complex challenges.

Our research helps clients to identify unique and sometimes hidden opportunities to 'nudge' the behaviour of customers, or users, towards a positive and often mutually beneficial goal. We do this using a variety of experimental techniques and the latest digital technologies."

19. CT's own marketing of its services, taken from their website and quoted above, demonstrates that the analysis and processing of personal data is key to their offerings and services to clients.

20. Taken together, it is likely that CT have processed personal data as part of their services to the Conservative Party. It would be very surprising if they did not, as what CT are transparent about is that their added value to their customers lies in their ability to analyse the electorate. Indeed, reports suggest that they were deployed to use these techniques in the 2019 General Election. For instance, *the Guardian* revealed[22] that CT were contracted by the Conservatives to conduct targeted advertising on Facebook and other social media platforms. It is not known what that involved or what data was used to conduct that targeting. However, as the Commissioner made clear in *Democracy Disrupted*, large pools of personal data are required for such targeting to work.

21. The latest returns, including spending for the Labour Party, were not released until December 2020 (while drafting these submissions). Privacy International are analysing those returns now and may revert to the Commissioner once we have had the opportunity to consider them in detail.

D. Privacy International's investigation

22. Privacy International has been concerned about the role of the political consultancy industry for some time, and in particular about their data processing activities and their approach to data subjects' rights.[23]

23. Privacy International has sought to examine the wider industry and their practices, with a particular focus on the 2019 general election. In doing so, Privacy International has considered electoral spending returns to ascertain which consultancies were used during that election.

[22] See, https://www.theguardian.com/politics/2019/oct/23/tories-hire-facebook-propaganda-pair-to-run-online-election-campaign and https://www.theguardian.com/politics/2019/oct/30/lynton-crosby-isaac-levido-protege-conservative-election-machine
[23] https://privacyinternational.org/long-read/4374/data-exploitation-and-political-campaigning-company-guide-resource

24. As explained above, Privacy International has analysed the spending returns from the Conservative Party as those returns were released in September 2020. We continue to analyse the returns for the Labour Party, which were released in December 2020.[24]

25. When considering the Conservative spending returns, Privacy International noted with concern the substantial but unparticularised role CT played in that election. Given CT's behavioural analytics offerings and services – and the personal data and profiling involved in such practices – Privacy International sought to investigate the role that CT may have played.

26. Privacy International conducted four stages of investigation into the practices of CT:

    i. Submitting data subject access requests, by members of our team who were registered voters for the 2019 general election, to which CT responded to say they held no personal data on those individuals;
    ii. writing to CT on 16 November, 2 and 16 December in an effort to illicit further information about their data practices and their role in the 2019 general election. CT did not respond to that correspondence – and at the time of writing, has still **not responded** to that correspondence (that correspondence is annexed to this complaint);
    iii. analysing the group of companies' privacy policies; and
    iv. researching the group of companies' publicly available marketing materials.

27. These investigative steps led to the material and documentation that forms the backbone of this complaint. However, those steps were necessarily limited to what CT has disclosed and as such, there is considerably further material that can and should be considered by the Information Commissioner. Given the increased scrutiny of the use of personal data in the democratic process it is

[24] https://privacyinternational.org/long-read/4374/data-exploitation-and-political-campaigning-company-guide-resource

concerning that neither we nor the public can fully understand the CT group of companies' role during the 2019 General Election.

E. Legal Framework and Concerns – Breaches of the DPA 2018 and GDPR

28. The very limited information available as to the data practices of CT demonstrates that its activities involve significant breaches of the Data Protection Act 2018 (**DPA**) and the General Data Protection Regulation (**GDPR**).

29. This submission is structured around four primary concerns about the data processing by CT, as revealed by the limited information that is available to PI:

    i. Identity of the data controllers
    ii. Transparency of processing activities
    iii. Legal bases for processing
    iv. Data subjects' rights

30. We address the concerns in turn.

I. Identity of the data controller

a. Background

31. As noted above, the spending returns for the Conservative Party from the 2019 General Election list "*CTF Partners Limited*" as a having conducted "*market research/canvassing*" for the Party. CTF Partners Limited are listed on Companies House with company number 07196537 and a registered address at 4th Floor 6 Chesterfield Gardens, London, England, W1J 5BQ. CTF Partners changed their name to **CT Partners Limited** on 25 August 2020.[25]

32. CT Partners Limited describe themselves as follows:[26]

[25] https://find-and-update.company-information.service.gov.uk/company/07196537/filing-history
[26] https://ctgroup.com/companies/#about

"C|T Partners is UK's leading campaign consultancy, combining cutting-edge research, high-level strategic advice and the latest tools in digital engagement.

Having delivered election success across multiple countries, at the very highest levels of politics, C|T knows the impact of timely information and the need to identify and focus resources. This is pivotal in everything that it does.

Applying hard-won lessons from decades of political campaigning, the team are specialists in advising major companies in how to position themselves to ensure they are integral to government decision-making, as well as providing calm strategic counsel in high-pressure situations.

Whether winning elections for prime ministers, or helping the world's leading businesses stay ahead, C|T Partners offers clients an unparalleled range of experience and an unrivalled record of success."

33. CT Partners Limited are within the group of companies operating under the umbrella of **CT Group**: https://ctgroup.com/. CT Group Limited is also registered in the UK, with company number 05893915 and registered office address is: Fore 1, Fore Business Park Huskisson Way, Stratford Road, Shirley, Solihull, West Midlands, B90 4SS.

34. Despite CT Partners Limited being named on the electoral spending returns and CT Group Limited acting as a parent company to CT Partners Limited, a third company, **CT Group Holdings Limited**, responded to subject access requests from Privacy International staff.

35. CT Group Holdings Limited are also registered with Companies House, with company number 10167550. CT Group Holdings Limited have the same registered office as CT Partners Limited: 4th Floor 6 Chesterfield Gardens, London, England, W1J 5BQ. CT Group Holdings Limited are the **only** entity registered with the Information Commissioner's Office, with registration number: ZA502118.

36. There are accordingly various companies involved in the data processing activities of concern. It is not clear on the face of the information Privacy International has been able to gather what the data processing relationship between these entities is (if any). Until the disclosures by the Electoral Commission, it was not clear which of the CT companies was engaged in UK elections (and it remains unclear whether the wider group fed into those services). It was also not made clear if CT Group Holdings Limited were answering the access requests on behalf of all companies.

b. Who are the controllers?

37. This corporate web obscures which of the three companies conducting the processing of the data is actually a data controller (or joint controller), and where, for example, data is being shared by one entity with another.

38. The spending returns for the 2019 General Election only list CT Partners Limited (then CTF Partners Limited) as being used by the Conservative Party. CT Partners Limited also make clear[27] that they conduct "*leading campaign consultancy, combining cutting-edge research, high-level strategic advice and the latest tools in digital engagement*."

39. Nevertheless, access requests could only be filed to a central administrative account of CT Group: enquiries@ctgroup.com. Privacy International staff submitted access requests to CT Group on 18 August 2020 and 25 August 2020. The response to that access request on 14 September 2020 (from: enquiries@ctgroup.com) was from CT Group Holdings Limited; a company not mentioned on the spending returns. Privacy International staff then submitted further requests on 9 November 2020, seeking access from CT Partners directly. The response to that further request was from the same email address, enquiries@ctgroup.com, without specifying who the response was on behalf of. There was thus no way for data subjects to make enquiries to CT Partners

[27] https://ctgroup.com/companies/#europe

Limited directly and CT Partners Limited did not respond to the initial access requests.

40. It is not therefore clear which of the three companies (i) processed personal data during the 2019 General Election, and (ii) continues to process personal data. It is unsatisfactory to have three separate companies listed as potentially involved in data processing activities (especially when only one company is registered with the Information Commissioner), for an unclear entity within the group of those companies to then respond to an access request. The Commissioner identified similar issues in respect of SCL / Cambridge Analytica around multiple companies and obscure inter-company data sharing as areas of particular concern. The same issues apply to the CT group of companies.

41. This problem is compounded by the failure to provide sufficient transparency over the data processing activities that one or more of the CT group companies are involved in.

II. Transparency

42. The three companies – Partners, Group, and Holdings – share a website. The website contains a "Privacy Notice", applying presumably to all the companies of the group and their data processing. That notice is available here: https://ctgroup.com/privacy-policy/. We refer to that privacy notice as 'the Notice' herein.

43. The Notice refers to "CT Group" only, without detailing which company (or companies) it refers to. A member of the public might assume that the reference is to CT Group Limited, but it is not clear if it also covers CT Group Holdings Limited and CT Partners. We accordingly refer to "CT" herein, to reflect the uncertainty of the scope of the notice.

44. In any event, the notice does not comply with Articles 13 and 14 GDPR. The notice does not adequately explain what the companies are doing with personal data, nor how data subjects are to exercise rights over that data. The net result

is "invisible processing".[28] The consequences for such invisible processing in the electoral process is particularly pronounced. As the Commissioner has acknowledged:[29]

> *"Trust and confidence in the integrity of our democratic processes risks being disrupted because the average person has little idea of what is going on behind the scenes.*
>
> *This must change. People can only make truly informed choices about who to vote for if they are sure those decisions have not been unduly influenced."*

a. Background

45. The notice sets out the scope of its application, confirming that it applies (emphasis added):

- "*to <u>your</u> use of any of our services where we are performing a data controller function;*
- *where <u>you apply to us</u> for a job or work placement;*
- *your <u>supply of services to us</u> where this involves any personal data; and/or*
- *to <u>any personal information collected from third parties</u> where we are the controller of such information.*"

46. This purports to be an exhaustive list of all processing activities that the companies are involved in. For the most part, the Notice is geared towards situations in which the individual reading the notice is the supplier of their own- or third-party data. Only the final bullet seems capable of covering campaign marketing or advice activities. The defining feature of the Notice is that it does not provide any proper transparency as to how CT process data in respect of such activities.

[28] ICO, What does 'invisible processing' mean?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when10
[29] https://ico.org.uk/about-the-ico/news-and-events/blog-information-commissioner-s-report-brings-the-ico-s-investigation-into-the-use-of-data-analytics-in-political-campaigns-up-to-date/

47. Indeed, the remainder of the notice is generic in nature and thus insufficient to inform an individual as to why and how their data has been processed. For example:

- The section "*how we collect your personal data*" is non-exhaustive when referring to third party sources. Rather, the Notice provides a series of examples of sources of data. This does not comply with a controller's obligations under the GDPR. Such non-compliance is particularly concerning in the context of 'invisible processing' in the political context. Given that most individuals would be unaware that CT is processing their data, it is essential that the controller provides more transparency, not less, as to its activities so that regulators like the Information Commissioner, and organisations such as PI can raise concerns on the behalf of data subjects. If an individual does look at the CT Notice, it is nigh on impossible for them to figure out if their data may be affected.

- CT does not specify a retention period for data. Rather, CT states that they "*retain the information we collect no longer than is reasonably necessary to fulfil the purposes that such data was originally collected in accordance with our internal data retention polices or to comply with our legal and regulatory obligations. A maintained copy of our retention policy is available upon request.*" That is not compliant with CT's obligations under the GDPR. A data subject should not need to ask for this retention policy. Further, when PI requested the policy, as described in paragraph 26(ii) above, CT did not provide it.

- CT does not specify the recipients or categories of recipients of any data that is shared. Rather, CT states that they "*may exchange your personal data with trusted, vetted, third-party service providers contracted to C|T Group*". CT also states that they will "*allow access to your personal data to the different entities within C|T Group's group*." As noted above, it is not

clear to data subjects which entities within the group are processing their data, and the basis upon which that processing is taking place.

- The reasons for sharing data with third parties are vague. The reasons cited include where a third party (emphasis added) "*require[s] such information, for example in fulfilling requests for information, receiving and sending communications, updating marketing lists, analysing data, providing support services or in other tasks from time to time*." This simply does not engage with the nature of the work of CT, and why and to whom they would share data (potentially sourced from unspecified third parties).

- CT confirms that personal data "*may be transferred to countries outside the EEA*". CT asserts that if they "*transfer your information outside the EEA in this way, we will take steps to ensure that your privacy rights continue to be protected*." This is far too broad.

48. Given the deficiencies within the notice, Privacy International wrote to CT on 16 November 2020. A copy of that letter is enclosed for the Commissioner's consideration (Annex A). In summary, the letter set out the defects in the notice and sought clarification of certain data processing activities. We further sought a copy of CT's data retention policies, in accordance with their stated policy. **CT did not reply to that letter.** At the time of writing, no reply has yet been received 67 days after it was first sent. PI also sent two additional reminder emails during this time, on 2 and 16 December 2020.

b. Legal/regulatory framework

49. Transparency is a core component of the first data protection principle, set out in Article 5(1)(a) GDPR. That principle requires data to be processed "transparently".

50. Articles 13 and 14 of the GDPR require a level of transparency as to how data is used. Recital (39) to the GDPR provides further clarity on the principles of transparency, stating (emphasis added):

"The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

51. The Article 29 Working Party Guidance on Transparency (Guidelines on Transparency)[30] explains the requirements of transparency under the GDPR as follows (emphasis added):

"the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that "[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data..." In particular, for complex, technical or unexpected data processing, WP29's position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should

[30] Guidelines on transparency under Regulation 2016/679 (WP260 rev.01)
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025

also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject?

52. Other aspects of the Guidelines on Transparency[31] also have direct application to CT's obligations:

    i. *"The "easily accessible" element means that the data subject should not have to seek out the information"* (para 11).
    ii. The following are "*Poor practice examples*" which "*are not sufficiently clear as to the purposes of processing":*
        - *"We may use your personal data to develop new services" (as it is unclear what the "services" are or how the data will help develop them);*
        - *"We may use your personal data for research purposes" (as it is unclear what kind of "research" this refers to); and*
        - *"We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails)."*

53. The Information Commissioner has also provided useful guidance on transparency[32]:

    i. The Commissioner states that transparency is about being "*clear, open and honest with people from the start about who you are, and how and why you use their personal data*."
    ii. Transparency is of heightened importance "*in situations where individuals have a choice about whether they wish to enter into a relationship with you*."

[31] Guidelines on transparency under Regulation 2016/679 (WP260 rev.01) https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025
[32] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

iii. The Commissioner confirms that transparency is (emphasis added) "*important even when you have no direct relationship with the individual and collect their personal data from another source. In some cases, it can be even more important - as individuals may have no idea that you are collecting and using their personal data, and this affects their ability to assert their rights over their data. This is sometimes known as 'invisible processing'*."

54. These guidelines are reinforced by enforcement action taken by the Commissioner. Of particular relevance is the enforcement action taken against Experian, which was in part precipitated by a complaint from Privacy International. In the enforcement notice against Experian, the Information Commissioner stated[33] that (emphasis added):

> *"Transparency is a key requirement of the GDPR. As part of this, individuals have the right to be informed about the collection and use of their personal data. This applies regardless of whether the personal data is obtained directly from the individual or from other sources. Organisations must be as transparent as possible about the personal data they are using, where they have obtained it from and the ways they will use it. They must be clear and upfront, explaining what they are doing in a way that individuals can readily understand."*

55. In the Commissioner's report on direct marketing,[34] the Commissioner highlighted that the need for transparency is greater where the controller has no active relationship with a data subject, as:

> *"If privacy information is not actively provided then this can cause 'invisible' processing – it is 'invisible' because the individual is not aware that the organisation is collecting and using their personal data."*

[33] https://ico.org.uk/media/action-weve-taken/enforcement-notices/2618467/experian-limited-enforcement-report.pdf
[34] https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf

56. Despite the clear legal transparency obligations set out in the legal framework, the Notice falls well short of what is required for CT to meet these obligations.

c. Application to facts

57. The Notice does not provide sufficient information for a data subject to know what data may be collected about them or how their data may be used by CT:

- Contrary to Articles 13(1)(a) and 14(1)(a) GDPR, the Notice does not identify the controller, as it refers to an entity that does not have legal personality. Moreover, the Notice refers to internal sharing of data within the group of companies, but does not describe nor define the respective data processing activities and role (controller, joint controller, processor) of each company.

- Contrary to Articles 13(1)(c) and 14(1)(c) GDPR, the Notice does not provide sufficient specificity of the purposes of the data processing. The Notice gives only generic purposes, with a non-exhaustive list examples. This is vague and *un*specific. Indeed, the Notice uses exactly the same or similar language as the "*poor practice examples*" cited in the Guidelines on Transparency[35] , such as "*provide you with C|T Group's services*". The lack of specificity of purposes also impacts on CT's ability to rely on the legal bases it refers to in the Notice, which is developed further below.

- Contrary to Articles 13(1)(e) and 14(1)(e) GDPR, the Notice does not specify the recipients or categories of recipients of personal data. Rather, the Notice refers in generic terms to data sharing with unspecified third parties. This is particularly pronounced where CT may have shared data with political parties, including the Conservative Party in the 2019 General Election. Privacy International further note reports[36] that CT subcontracted certain services, including targeting of adverts.

[35] Guidelines on transparency under Regulation 2016/679 (WP260 rev.01) https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025
[36] https://www.theguardian.com/politics/2019/apr/03/grassroots-facebook-brexit-ads-secretly-run-by-staff-of-lynton-crosby-firm ; https://www.theguardian.com/politics/2019/aug/01/revealed-johnson-allys-firm-secretly-ran-facebook-propaganda-network

- Contrary to Articles 13(1)(f) and 14(1)(f) GDPR, the Notice, while confirming that data may be transferred out of the EEA, does not provide a "*reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available*."

- The Notice does not specify the retention periods applicable. Rather, CT requires data subjects to request a copy of the relevant retention policies. Despite Privacy International asking for those policies, they were not provided. A data subject cannot therefore know the retention periods for their data, contrary to Articles 13(2)(a), or at a minimum the criteria used to determine the periods, contrary to 14(2)(a) GDPR. This failure to have clear and precise retention policies means CT cannot also demonstrate compliance with Articles 5(1)(c) and 5(1)(e) GDPR.

- It is not made clear if CT are involved in profiling. The reports[37] of what CT did during the 2019 General Election would suggest that they were involved in some form of profiling, in order to be able to target people with adverts. If so, CT have contravened Articles 13(2)(f) and 14(2)(g) GDPR as the Notice does not inform the data subjects of such profiling.

- Contrary to Article 14(2)(f) GDPR, CT do not specify the sources of the personal data they process, and if applicable, whether it came from publicly accessible sources.

58. Under Article 5(2) GDPR, CT have the burden of showing compliance with the data protection principles. As set out above, CT are not processing data transparently and are in breach of Article 5(1)(a) GDPR.

59. Privacy International's core, overarching, concern is that CT group is involved in what the Information Commissioner refers to as "invisible processing". The Commissioner cited this as of particular concern in the enforcement notice

[37] https://www.theguardian.com/politics/2019/apr/03/grassroots-facebook-brexit-ads-secretly-run-by-staff-of-lynton-crosby-firm; https://www.theguardian.com/politics/2019/aug/01/revealed-johnson-allys-firm-secretly-ran-facebook-propaganda-network

against Experian. Given CT seem to have been involved in processing of data for political ends and that such invisible processing will have effects on democratic participation, the use of such data should be subject to increased transparency.

60. The Article 29 Working Party has been clear that the more intrusive (or less expected) the processing is, the more important it is to provide information to individuals in advance of the processing (in accordance with Articles 13 and 14 GDPR). The onus should not be on individuals to trawl through the privacy policies of these companies or to make access requests in order to receive information about how their data is being processed. This is why, as set out above, the CT group has failed to comply with these obligations.

III. Legal bases

61. For the processing of personal data to be "*lawful*" for the purposes of Article 5(1)(a) GDPR, at least one of the conditions under Article 6 GDPR must apply. The legal bases cited by CT for all processing activities they are undertaking are contained within the Notice.

62. The Notice refers to four potential legal bases for processing of personal data: (i) legitimate interests (ii) consent (iii) compliance with a legal obligation and (iv) performance of a contract. We address each in turn, in respect of data subjects whose data may have been processed by CT during the 2019 General Election.

i. Legitimate interests (Article 6(1)(f) GDPR)

63. CT state that they rely on legitimate interests where they "*consider use of your information as being (a) non-detrimental to you, (b) within your reasonable expectations, and (c) necessary for our own, or a third party's legitimate purpose*." This must be a core legal basis to the processing activities engaged in during the 2019 General Election as, to the best of Privacy International's knowledge, most voters will not have a direct relationship with CT group.

The law

64. Article 6(1)(f) provides the framework for reliance on legitimate interests, stating that processing will be lawful only so far as:

> *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

65. Recital (47) provides context to this provision (emphasis added):

> *"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data*

for direct marketing purposes may be regarded as carried out for a legitimate interest."

66. Recital (47) thereby confirms that controllers should consider the expectations of data subjects when assessing whether their legitimate interests are outweighed by the interests of data subjects. The interests and fundamental rights of data subjects "*could in particular override*" that of the controller where data subjects "*do not reasonably expect further processing*." Most obviously, data subjects would not reasonably expect further processing if that processing is "*invisible"*.

67. The Commissioner has provided detailed guidance[38] on how to apply legitimate interests in practice. In its explanation of how legitimate interests as a lawful basis works in practice, the Commissioner flags that:

    a. It is likely to be most appropriate where the controller uses people's data in ways they would reasonably expect, and which have minimal privacy impact, or where there is a compelling justification for the processing.
    b. If a controller chooses to rely on legitimate interests, the controller is taking on extra responsibility for considering and protecting people's rights.
    c. Legitimate interests may be a ground for marketing purposes <u>if</u> the controller can show that how they use people's data is proportionate, has a minimal privacy impact, and that data subjects <u>would not be surprised</u> or likely to object.
    d. The controller should keep a record of their legitimate interest assessments.
    e. The controller must include details of legitimate interests in privacy information.

68. The Commissioner's guidance also states that:

[38] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them.

69. The Commissioner states that if a controller does rely on 'legitimate interest', those 'interests' should be clear and specific.

70. The Commissioner suggests that controllers should apply a three-stage test when determining the application of legitimate interests:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

71. This test should also be conducted before the processing begins.

Application to facts

72. CT do not explain how they balanced the impact of their processing activities against the rights of individual data subjects. As the Information Commissioner stated in the investigation into direct marketing,[39] any reliance on legitimate interests must be supported by an assessment of those interests against the impact on data subjects. There is no evidence from the Notice that the required analysis has been undertaken.

73. In any event, it is difficult to see what the benefit to individual data subjects could be for CT processing their data, such to justify the balance being struck in favour of CT's continued processing over the rights of data subjects. The only conceivable processing activity of benefit that CT can point to is to provide direct marketing and communication to individuals. As the Commissioner has stated in her own guidance – and emphasised in the enforcement notice against Experian:

[39] https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf

"Little weight can be attached to supposed benefit of the data subject consumer receiving direct marketing communications more 'appropriate' to them, when this is a consequence of processing and profiling to which they have not consented. The Commissioner considers that it is unlikely that a controller will be able to apply legitimate interests for intrusive profiling for direct marketing purposes. This type of profiling is not generally in an individual's reasonable expectations and is rarely transparent enough."[40]

74. These same considerations apply to the processing CT conducts. As detailed above, CT are involved in processing for political ends. That processing is likely to involve processing of profiled data – whether directly or through third parties – which cannot be presumed to fall within individuals' reasonable expectations. The lack of foreseeability is compounded by the transparency problems detailed above. As such, any legitimate interest assessment would fall in favour of the data subjects.

75. Privacy International agree with the Commissioner's findings in respect of legitimate interest assessments conducted by the data-broker industry and request that the same scrutiny and requirements be applied to the political consultancy industry. In the Experian investigation, the Commissioner found[41] that all of Experian's assessments had concluded in favour of processing, as they had not been properly weighted. Any assessments conducted by CT and other political consultancies should be scrutinised in the same way, as nothing so far indicates that CT's assessments (if any were conducted) concluded against processing.

ii. Consent (Article 6(1)(a) GDPR)

76. The Notice states

[40] Enforcement notice against Experian, para 58 (https://ico.org.uk/media/action-weve-taken/enforcement-notices/2618467/experian-limited-enforcement-report.pdf)
[41] https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf

"You may be asked to provide your consent in connection with certain services that we offer, for example in respect of any processing of your personal data for our marketing purposes where you or your employing organisation is not a client of C|T Group, or in respect of certain special categories of personal data such as your health or racial background for which we are legally obliged to gain your consent due to the sensitive nature of such information and the circumstances in which it is gathered or transferred. Where we are reliant upon your consent, you may withdraw this at any time by contacting us in accordance with the section 15 (Further information) below, however please note that we will no longer be able to provide you with the products or services that rely on having your consent."

77. CT were used by the Conservative Party to conduct "*market research*"[42] during the General Election. As the Notice expressly refers to "*marketing purposes where you or your employing organisation is not a client of C|T Group*", CT would appear to be relying on consent for at least part of their processing during the 2019 General Election. It is unclear how this consent was obtained.

The law

78. The burden of demonstrating that consent has validly been provided by data subjects rests with the controller, under Article 7(1) GDPR. Consent is defined in Article 4(11) GDPR as "*freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

79. Recitals (42) and (43) GDPR provide some further context to the requirements of consent:

"(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context

[42] As detailed in the spending returns.

of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC ([10]) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

80. In addition to these base requirements, Article 7 GDPR specifies further conditions for consent. Elements that are germane to CT include:

- Consent should not be buried or bundled within other terms when given as part of a written declaration. Rather, such consent must be "*clearly distinguishable from the other matters*" within that written declaration.
- Data subjects must be afforded the right to withdraw consent. The data controller is obliged to make it "*as easy to withdraw as to give consent*."

81. The European Data Protection Board Guidelines on Consent[43] provide a helpful overview of what these requirements mean in practice:

a. **Freely given** – This means there must be "*real choice and control for data subjects*"[44]. Such free choice may be impacted where there is an imbalance of power between the data controller and the data subject. Real choice would also be undermined if consent is made conditional or that consent is not sufficiently granular (i.e. the data controller does not conflate purposes for processing).
b. **Specific** – The Guidance on Consent confirms that "*The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject*." In turn, the Guidance on Consent suggests tha "*to comply with the element of 'specific'*" the data controller "*must apply: (i) Purpose specification as a safeguard against function creep, (ii) Granularity in consent requests; and (iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters*"[45].
c. **Informed** – The Guidance on Consent provides "*Minimum content requirements for consent to be 'informed'*"[46]. This is information that must be provided to ensure that a data subject is sufficiently "*informed*" in order for consent to be validly given. The guidelines also state that where "…*the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named*."
d. **Unambiguous indication of the data subject's wishes** – this is where an individual, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject must have taken a deliberate action to consent to the particular processing.

82. The Guidance on Consent highlights that (sic):

[43] Guidelines 05/2020 on consent under Regulation 2016/679 (4 May 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[44] At para 13
[45] At para 55
[46] At para 64

> *"Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49, and in Article 22 on automated individual decision-making, including profiling."*[47]

Application to facts

83. It is difficult to reconcile CT's invisible processing with data subjects providing "*specific, informed and unambiguous*" indication of their wishes for their data to be used as CT did during the 2019 General Election.

84. In particular, CT is not transparent about their processing. It is not clear what data processing was undertaken during the 2019 General Election. If CT did process any personal data during that election, such processing is unlikely to have been conducted based on lawful consent. Individual data subjects are indeed unlikely to have even heard of CT, let alone interacted with them in any way such to provide specific, informed and unambiguous consent. As such, consent is unlikely to be sufficient as a legal basis under Article 6 GDPR – if, indeed, CT relies on it for this purpose. The problem is, as highlighted above, it is unclear what bases are relied upon for the specific types of activities CT engaged in on behalf of the Conservative party.

Special category data

85. Special category data is protected by Article 9(1) GDPR:

> *"Processing of 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*

[47] At para 91

uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

86. Thus, processing of such special category data is prohibited. A data controller can only process such data if one of the exemptions in Article 9(2) GDPR apply.

87. The ICO guidance[48] on the processing of such special category data explains why such data deserves extra protections:

> *"It's not just that this type of information might be seen as more sensitive or 'private'. The recitals to the UK GDPR explain that these types of personal data merit specific protection. This is because use of this data could create significant risks to the individual's fundamental rights and freedoms.*
>
> *…*
>
> *The presumption is that this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination."*

88. As detailed in Recital (51) GDPR,

> *"Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms."*

89. The ICO similarly recognise that "Special category data is the most sensitive personal data a controller can process. The misuse of this data is likely to interfere with an individual's fundamental rights and freedoms and could cause real harm and damage."[49]

[48] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/
[49] https://ico.org.uk/about-the-ico/news-and-events/blog-why-special-category-personal-data-needs-to-be-handled-even-more-carefully/

90. Data revealing of political opinions falls within such “special category data”. The European Data Protection Board recognised the “serious risks” that the processing of data revealing political opinions during electoral cycles presents[50]:

> *Predictive tools are used to classify or profile people’s personality traits, characteristics, mood and other points of leverage to a large extent, allowing assumptions to be made about deep personality traits, including political views and other special categories of data. The extension of such data processing techniques to political purposes poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process.*

91. It is not clear if CT processed data revealing political opinions, owing to the defective transparency notices. If they did so, they would be processing special category data, which is prohibited under Article 9(1) GDPR. The only relevant exemption to do so would be by receiving “explicit consent” under Article 9(2)(a) GDPR.

92. If CT have been processing data revealing political opinions – which seems inevitable given their role in the 2019 General Election – it is not clear how they would have received consent for such processing from data subjects. The processing of data revealing of political opinions – and the lawful basis for such processing – is of critical importance when scrutinising the work of CT and the wider role of political consultancies.

93. Thus, the processing of data that may reveal political opinions by CT requires particular scrutiny, given the “*serious risks … to trust in the integrity of the democratic process*” created by invasive political profiling activities. Accordingly, the ICO should scrutinise whether CT are processing special category data. If so, the ICO must anxiously scrutinise CT’s claimed lawful basis for the processing of any special category data, including, in particular, data revealing

[50] Statement 2/2019 on the use of personal data in the course of political campaigns (13 March 2019)

of political opinions. Short of explicit consent, it is difficult to envisage any lawful basis for such processing.

iii. *Performance of a contract (Article 6(1)(b) GDPR)*

94. CT state:

> *"We may need to collect and use your personal data to enter into a contract with you or to perform a contract that you have with us, and where we respond to your requests and provide you with services in accordance with our terms and conditions (which are available on request) or other applicable terms of business agreed with you or with your employing organization."*

95. This lawful basis for processing is not applicable to individuals who do not have a relationship with CT. Rather, it would only apply to entities that have a contractual relationship with CT. While this may be applicable to focus group members, this would not apply to the wider electorate as data subjects.

iv. *Compliance with a legal obligation (Article 6(1)(c) GDPR)*

96. This base only applies to very limited data processing activities. Those activities appear irrelevant to the data processing involved in the 2019 General Election.

v. *Conclusion*

97. Taken together, the legal bases cited by CT, analysed on the basis of the limited information available to us, are insufficient to show that data has been processed lawfully which is a contravention of Article 5(1)(a) GDPR.

IV. Rights of data subjects

98. The problems with the Notice detailed above have consequent effects for data subjects' rights. In particular:

i. The legal bases cited by CT are unclear. As such, a data subject cannot appreciate which legal basis applies to which purpose of processing.

This is not only a contravention of Articles 13(1)(b) and 14(1)(b) GDPR (as detailed above), but also impairs the exercise of certain rights. For instance, a data subject cannot exercise their right to erasure under Article 17 GDPR as that right is related to the legal basis for processing. Likewise, a data subject will only be able to object under Article 21 GDPR to processing that is conducted pursuant to the either processing in the public interest or legitimate interests as an identified legal basis. CT do not rely on public interest as a legal basis for processing. However, it is not clear which legal basis CT relies upon for its different processing activities and as such, a data subject cannot know which processing purposes they could object to under Article 21 GDPR.

ii. The retention policies are not provided to data subjects within the Notice. Rather, a data subject has to ask for those policies. When Privacy International requested those policies, CT did not respond.

iii. In response to access requests by Privacy International staff, CT responded to state that CT Group Holdings did not process any information. No response was provided in respect of CT Partners Limited, despite this being the company listed on the Conservative's General Election spending returns. It is therefore not clear what data CT Partners process or how a data subject is to exercise rights over that data.

99. These are examples of the problems that data subjects face. Those problems are aggravated by the lack of transparency about (i) who the controllers are and (ii) what data is being processed as detailed above.

100. In these circumstances, data subjects require greater control over the data being processed by CT. In the same way that the Commissioner sought greater control for data subjects over data held by Experian and other data broker companies, Privacy International requests the Commissioner to take action against CT and others within the political campaigning consultancy industry.

F. Remedies

101. The Information Commissioner continues to investigate the use of data by political parties as part of the ongoing audit of the use of data in the democratic process. Privacy International welcomes that continued engagement by the Commissioner.

102. As the Commissioner has recognised, political parties rely on third parties to assist with their data analytics, profiling and marketing activities. Those third parties are often not transparent about their use of personal data.

103. As set out above, the CT group of companies were involved in the 2019 General Election. The electoral spending returns list CT as conducting marketing and research. Reports of CT's activities suggest that marketing and research included direct targeting of individuals for political advertising. Despite that role, CT do not adequately explain how they collect and what they do with personal data. Rather, CT appear to be involved in "*invisible processing*".

104. In this context, there are a number of aspects of CT's data processing activities that the Commissioner should consider. Privacy International suggests that the Commissioner conduct such inquiries as part of the Commissioner's ongoing work into political data. In particular, Privacy International invites the Commissioner to consider:

    i. Who the relevant **data controllers** are within the CT group of companies;
    ii. The **transparency principle** in relation to how CT use personal data;
    iii. The **lawfulness principle** in relation to how CT process personal data. In particular, CT's reliance on legitimate interests as a lawful basis for processing is questionable;
    iv. An assessment of whether CT process **special category data**, including data relating to political opinions and special category data used for

electoral purposes. If so, whether CT have an appropriate legal basis for such processing; and

v. **Data subject rights**, in particular the right of access and rights to erasure and objection.

105. Given the issues raised in this submission, Privacy International strongly encourages the Commissioner could commence any such enquiry through an assessment notice of CT pursuant to section 146 DPA.

106. Any such review should be considered as part of a review into the wider political consultancy industry and would be key to ensuring that the Commissioner's review of political data is holistic and targeted at all those involved in such processing.

PRIVACY INTERNATIONAL

21 January 2021

Annex A

16th November 2020

C|T Group Ltd
6 Chesterfield Gardens
Mayfair
London W1J 5BQ
United Kingdom
+44 (0) 20 7318 5770
dataprotectionoffice@ctgroup.com
Enquiries@ctgroup.com

Dear Sir/ Madam,

I am writing on behalf of Privacy International.

We write in respect of the personal data the CT group of companies[1] processes. We refer to the CT group of companies as "CT" herein to avoid confusion, save where we refer to a specific CT entity.

Background

Privacy International (PI) is a London based non-governmental organisation that works globally at the intersection of modern technologies and human rights. As part of our programme of work on "Defending Democracy and Dissent", we campaign to improve regulatory safeguards against political data exploitation by advocating for enforcement of existing safeguards and the introduction or reform of others.

The first batch of campaign spending data recently published by the Electoral Commission in relation to the 2019 UK General Election shows CT Partners Ltd (operating under the name CTF Partners Ltd during that election) as one of the major providers of market research and other

[1] We understand that the CT Group of companies is made up of CT Group Ltd (05893915), CT Group Holdings Ltd (10167550) and CT Partners Ltd (07196537). We see the ICO registered controller is CT Group Holdings. However, we note in contrast from your privacy notice that CT Group is named as the data controller, albeit the actual data controller is not clear. See further below.

services during this election. In particular, the campaign spending returns suggest that CT Partners Ltd working for the Conservative and Unionist Party (referred to as the "Conservative Party" herein).

We write to request information about CT's data processing activities and CT's involvement in the 2019 election.

Transparency requirements

The Information Commissioner's Office have stated in recent enforcement actions[2]:

> *Transparency is a key requirement of the GDPR. As part of this, individuals have the right to be informed about the collection and use of their personal data. This applies regardless of whether the personal data is obtained directly from the individual or from other sources. Organisations must be as transparent as possible about the personal data they are using, where they have obtained it from and the ways they will use it. They must be clear and upfront, explaining what they are doing in a way that individuals can readily understand.*

To this end, Articles 13 and 14 of the General Data Protection Regulation (GDPR) require a level of transparency as to how data is used.

We have considered CT's privacy notice in full (referred to as the "Notice" herein). That Notice does not provide sufficient information for a data subject to know what data may be collected about them or how their data may be used by CT. For example, the Notice does not provide clarity on (1) who CT receive data from (2) what CT do with data. We address those two examples in turn, before turning to specific questions about CT's data processing activities.

1. Sources of data

Article 14 GDPR requires that where organisations obtain personal data from sources other than the individual, they must provide privacy information to individuals within a reasonable

[2] ICO *Investigation into data protection compliance in the direct marketing data broking sector* (Oct 2020) available at: https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf

period, and at the latest within a month of obtaining their data. The Information Commissioner has particular concerns with such processing[3]:

> *If privacy information is not actively provided then this can cause 'invisible' processing – it is 'invisible' because the individual is not aware that the organisation is collecting and using their personal data.*

CT appear to be involved in such "invisible processing", particular with respect to political campaigning activities. Individual data subjects are unlikely to have a direct relationship with you. The personal data CT collect seems to be instead obtained from other sources rather than directly from individuals. As such, CT are accordingly required to provide greater transparency over that data. The Notice does not meet these transparency requirements.

There is also a disconnect between the electoral spending returns – which suggests CT conducted data processing for the Conservative Party – and the Notice. The Notice does not sufficiently explain how that data was collected, what sources were used, how it was processed or how the data was used.

2. Why CT are collecting data

The Notice is limited to examples of reasons why CT collect data only. CT state, "We use your information in order to provide you with, and improve, our services, for example" and then provide a list of generic examples. No further information is provided. The Article 29 Working Party Guidance on Transparency provides examples of "poor practice" that would violate the requirements of the GDPR. This includes the following examples of particularly poor practice:

> "*We may use your personal data to develop new services" (as it is unclear what the "services" are or how the data will help develop them);*

This "poor practice" phraseology from the Guidance mirrors the phrasing used in the Notice. Thus, the Notice is inadequate to meet the basic transparency requirements in the GDPR.

3 *Ibid.* See also: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

Questions

As detailed above, the Notice does not provide transparency for a data subject to know what data has been collected nor what happens with such data.

As part of our efforts to assist data subjects with understanding how their data is used, we would like to gain a fuller picture of the services provided to political parties, and how CT use data. Therefore, we would be very grateful if you could answer some questions in relation to how CT processes personal data.

We have questions in respect of both (1) the Notice and (2) CT's role in the 2019 election. We address each in turn.

I. <u>The Notice</u>

1. Can you please explain who the data controllers are? We note the Notice refers to "C|T Group" but does not mention CT Partners. In contrast, the only CT entity registered with the ICO is CT Group Holdings Limited (registration number: ZA502118). Please explain the relationship between these various entities (and any other company within the CT group of companies) and whether they act as joint controllers of personal data. Please also explain whether the named data controller on the Notice, CT Group, is the entity registered with the ICO?

2. The Notice states that CT will "exchange your personal data with trusted, vetted, third-party service providers". Please clarify who those third parties are?

3. The Notice allows for the "disclosure of information" to third parties where "sharing is provided for under contract". Can you please clarify if this refers to the contract between CT and a data subject or the contract between you and the third party?

4. Your retention periods are not specified in the Notice but will be "provided on request". Please provide those retention policies.

5. Please provide a full list of all purposes for why CT collect data, with associated legal bases.

II. The 2019 Election

1. What services did CT provide during the 2019 election? Did CT process any personal data (including collected, retained, shared, stored or otherwise made available) for these services and if so for which services?

2. The electoral spending returns from the Conservatives states you conducted "marketing research/canvassing services". Please clarify what this means and what it entails?

3. What were the sources of this data? Please specify particularly whether:
    a. CT collected the data and if yes, from which sources. Did you collect data directly from individuals or through other sources, such as social media profiles or the voter register;
    b. CT bought data from third parties, such as data brokers, credit reporting agencies. If yes, could you specify which companies you bought data from?

4. Did any of the services provided involve any processing of personal data? If so,
    a) What are the categories of personal data, including any metadata[4], processed by CT Partners for the elections? Please list the specific categories.
    b) Please provide a list of the special-category personal data processed by CT Partners, such as personal data revealing, among others: nationality, information contained in asylum applications or applications for international protection, 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 revealing criminal convictions or offences.
    c) Please clarify the extent of the data you held. In particular, did you have the Conservative Party's database or had access to it? Did you analyse the data from the Conservative Party's database?
    d) Further, did you analyse the electoral record in full?

5. For each category of personal data and/or personal data, please explain:
    a. The purpose(s) of the processing;
    b. The legal basis for the processing;

[4] By metadata, we refer to any data other than content, including who, when and where of a communication.

i. If the legal basis for processing is consent, demonstrable evidence of the date and how consent was provided;
ii. If the legal basis for processing is legitimate interest, did CT Partners carry out a legitimate interest impact assessment? If so, please explain whether those impact assessments ever resulted in you ceasing processing.
iii. When receiving data from third parties, if you ever verified or considered that third parties' legal basis for processing.
iv. When you receive such third-party data, what is the lawful basis for that data once received?

6. Was any personal data used for profiling?
    a. Did CT Partners merge data from different sources into profiles, and if yes which sources?
    b. If yes, please specify the legal basis for profiling as well as whether a data protection impact assessment was carried out?

7. Was any of the personal data used for automated decision making? If so, please provide the meaningful information about the logic involved, as well as the significance and the envisaged consequences?

8. Does CT Partners process any non-personal data? If yes, please list the categories of non-personal data that may be processed? Does CT Partners, for example, process any aggregated data, anonymised or pseudonymised data? If so, does CT Partners control or process the processed non-personal data?

9. Was the data processed during the elections deleted after the elections have taken place? If not, why not? Was the same data used for other purposes?

10. Was any of the data shared with any third party, including, but not necessarily limited to political parties? If yes, please provide specific details about each recipient, the data shared with them, the purpose(s) and legal basis for sharing, as well as the details of the agreement entered into for this sharing.

11. Has any personal data transferred outside the EU? If yes, what measures have been taken for their protection?

12. Was there a Data Protection Impact Assessment done in relation to each of the CT Partners services provided during the elections? If yes, please provide a copy of the Data Protection Impact Assessment Reports. If not, please explain why.

13. Has the Information Commissioner's Office (ICO) been notified in relation to any data processing by CT, including by communicating Data Protection Impact Assessments (DPIAs) to it and/or seeking its views on data processing matters in relation to CT's processing of data?

We will assume that any response provided to us may be published unless otherwise notified.

Many thanks in advance for helping us gain a fuller picture of the services provided during elections, and how CT uses data.

We would be very grateful to receive a response within 7 days from the date of this letter, by 23rd November 2020.

Yours faithfully,

Lucy Purdon
Policy Director
Privacy International
[redacted]

CC. Ilia Siatitsa, Legal Officer, Privacy International