Version: 1
Date: 1 June 2018

Protocol for dealing with claims of privacy rights in connection with unannounced searches conducted on foot of a search warrant under section 36 or section 37 of the Competition and Consumer Protection Act 2014

1. INTRODUCTION

1.1. This document is a protocol (the "Protocol") which sets out the safeguards adopted by the Competition and Consumer Protection Commission (the "CCPC") for the purpose of respecting the privacy rights of businesses and individuals before, during and after the conduct of unannounced searches of business premises or private dwellings on foot of a search warrant under section 36 or 37 of the Competition and Consumer Protection Act 2014 (the "2014 Act").

1.2. In particular, the Protocol sets out a process (at Sections 4 and 5 of the Protocol) for dealing with claims made to the CCPC by the undertaking or individual who is the target of the CCPC's search operation (the "Search Target"), either during the course of the search or following its completion, that certain material which was forensically copied or seized by authorised officers of the CCPC during the search contains private information.

1.3. The process set out in this Protocol is to be used for the identification by the Search Target of material that it claims contains private information and the verification by the CCPC of those claims. For the purpose of the Protocol, the CCPC considers "**private information**" to be information relating to an undertaking or individual which does not concern the business or economic activities or interests of such undertaking or individual. For the avoidance of doubt, business or economic activities are activities relating to the business of supplying or distributing goods or providing a service.

1.4. The process set out in this Protocol is not applicable to claims that the CCPC has seized or forensically copied material which is protected by legal professional privilege. The CCPC has put in place a separate process for dealing with material over which a claim of legal professional privilege has been made. It is the intention of the CCPC that its policy in relation to legal professional privilege claims will be more fully outlined in a separate protocol which will be published on the CCPC's website.

2. CCPC'S SEARCH PREPARATION AND PLANNING

2.1. Under section 37 of the 2014 Act, authorised officers of the CCPC investigating a suspected breach of competition law under the Competition Act 2002 may, on production of a warrant issued by the District Court pursuant to section 37(3) of the 2014 Act, conduct an unannounced search of an undertaking's business premises and/or the home of any relevant director, manager or member of staff of the undertaking. During a search, the authorised officers have various powers, including (but not limited to) the power to: seize and retain books, documents and records; take copies of books, documents and records; and require any person present to provide books, documents and records in that person's power or control to the authorised officers.

2.2. Under section 36 of the 2014 Act, authorised officers of the CCPC have powers of inspection for the purpose of enforcing consumer protection law and other relevant statutory provisions. During such inspections, authorised officers of the CCPC may exercise various powers without a warrant, including (but not limited to) the power to: conduct an unannounced search of a business premises; inspect and take copies of books, documents and records; and require any person present to produce books, documents and records in that person's power or control to the authorised officers. In the context of such inspections, the authorised officers may remove books, documents or records from the business premises or conduct a search of a private dwelling only on foot of a warrant issued by the District Court pursuant to section 36(4) of the 2014 Act.

2.3. If, during the course of a CCPC investigation, the CCPC case team decides to conduct an unannounced search on foot of a warrant under section 36 or 37 of the 2014 Act in order to obtain information which may be relevant to its investigation, the CCPC will designate a search team for the purpose of carrying out the search of the identified business premises or private dwelling.

2.4. The CCPC seeks to ensure that a proportionate approach is taken when conducting searches. To this end, the search team takes steps during the planning phase to ensure that the search operation will be as focused as possible and that it targets the individuals (i.e. persons of interest) and information sources that are potentially relevant for the purposes of the investigation.

2.5. The search team will generally meet periodically in the lead up to the search operation in order to discuss the operational plan for the search. The issues discussed at meetings of the search team will typically include: the search site; the strategy on entry; the types of evidence which are potentially relevant to the CCPC's investigation and which the search team will look for; and the devices, locations, individuals and custodians which may hold material that is potentially

relevant to the CCPC's investigation and which the search team will focus on for the purpose of the search.

2.6. In the lead up to the search operation, members of the CCPC's Digital Investigations Unit will generally also attend meetings with the search team and assist the search team in identifying persons of interest and the likely electronic devices that such individuals may use. The Digital Investigations Unit may utilise open source forensic tools as well as other sources for the purpose of gathering as much information as possible in order to help the search team to prepare for the search operation and to search the identified business premises or private dwelling in a targeted way.

2.7. During these meetings, the search team may also develop and refine keywords and other search parameters based on the nature of the CCPC's investigation that may be used during the search operation to ensure that the search remains focused and that only potentially relevant material, individuals and custodians of data are identified for the purpose of the search. A range of keywords and other search parameters may be applied to electronic material at the search site as well as to electronic material seized or forensically copied at the search site which is subsequently interrogated offsite at the CCPC's offices. These keywords and other search parameters used by the CCPC may evolve over the lifetime of the CCPC's investigation. A record of the keywords and other search parameters used throughout the CCPC's investigation will be maintained by the search/case team.

2.8. Following the receipt of any necessary internal approvals, a designated authorised officer of the CCPC will make an application to the District Court for a search warrant or warrants under section 36(4) or 37(3) of the 2014 Act. Such authorised officer will attend before a District Court judge and provide the judge with information on oath which demonstrates to the judge that there are reasonable grounds for suspecting that evidence of, or relating to, the commission of an offence under the relevant legislation is to be found at the place for which the search warrant is sought. Where the judge is satisfied that there are reasonable grounds for suspecting that evidence of, or relating to, the commission of an offence under the relevant legislation is to be found in the place identified by the authorised officer, he/she may issue a warrant authorising the entry and search of such place, using reasonable force where necessary, at any time or times within one month from the date of issue of the search warrant, and the exercise of all or any of the powers conferred on an authorised officer under section 36 or 37 of the 2014 Act during the course of that entry and search.

3. INFORMATION GIVEN BY THE CCPC TO THE SEARCH TARGET REGARDING THE SCOPE OF ITS INVESTIGATION

3.1. In all instances where the CCPC conducts an unannounced search on foot of a search warrant under section 36 or 37 of the 2014 Act, the CCPC authorised officer to whom the search warrant has been granted (the "Warrant Holder") will – at the outset of the search operation – produce the original search warrant to the person in charge at the search site. The person in charge at the search site will be given a sufficient opportunity to review the search warrant.

3.2. In the majority of cases, the Warrant Holder will also give the Search Target a photocopy of the search warrant at the outset of the search operation. However, if the Warrant Holder has concerns that attempts may be made by the Search Target to interfere with potential evidence at the search site or to pass information to the targets of other searches being conducted by the CCPC at the same time, or for other operational reasons, a photocopy of the search warrant will be given to the Search Target at a later stage in the search operation once the Warrant Holder is satisfied that potential evidence at the search site and any other relevant search site(s) has been secured and that any other operational issues have been resolved.

3.3. At an early stage in the search operation, the Warrant Holder may also provide the Search Target with an explanatory note describing the purpose of the search, including the suspected anti-competitive conduct being investigated by the CCPC and the type of material that is being sought under the search warrant. However, if the Warrant Holder has concerns that attempts may be made by the Search Target to interfere with potential evidence at the search site or to pass information to the targets of other searches being conducted by the CCPC at the same time, or for other operational reasons, the explanatory note will be given to the Search Target at a later stage in the search operation once the Warrant Holder is satisfied that potential evidence at the search site and any other relevant search site(s) has been secured and that any other operational issues have been resolved.

3.4. The CCPC considers that the abovementioned measures ensure that the Search Target has access – during the search operation – to information that it needs regarding the nature and scope of the CCPC's investigation.

4. CLAIMING PRIVACY RIGHTS DURING A CCPC SEARCH OPERATION

A. Raising privacy concerns with the Warrant Holder

4.1. If, during the course of a search operation, the Search Target has concerns that certain material (whether in hard copy or electronic format) contains private information and should not be reviewed or forensically copied/seized by the CCPC authorised officers, these concerns should be communicated to the Warrant Holder together with reasons as to why the material in question is considered to be private. As noted in paragraph 1.3 above, the CCPC considers "private information" to be information relating to an undertaking or individual which does not concern the business or economic activities or interests of such undertaking or individual.

4.2. The CCPC considers that the CCPC authorised officers have the right to inspect any and all business-related books, documents or records, whether in hard copy or electronic format, during the search operation (with the exception of any material over which a claim of legal professional privilege has been made). This includes the right to check whether books, documents or records found at the search site are actually business-related documents. If the CCPC authorised officers consider that any of the hard copy or electronic material in relation to which the Search Target has expressed privacy concerns may contain information that is potentially relevant to the CCPC's investigation, the CCPC authorised officers will proceed to seize or forensically copy such material subject to certain safeguards described in the paragraphs below.

B. Privacy claims raised in respect of electronic material

4.3. In relation to **electronic material** (e.g. electronic devices, electronic files and other electronic documents) claimed by the Search Target to be private but which the CCPC authorised officers consider may contain information potentially relevant to the CCPC's investigation, the Warrant Holder will explain to the Search Target that the electronic material in question will be seized or forensically copied by the CCPC. However, such electronic material will be kept separate from other electronic material seized or forensically copied by the CCPC over which no privacy claim has been made by the Search Target (unless the electronic material over which privacy has been claimed by the Search Target cannot be separated from other electronic material over which privacy has not been claimed – see paragraph 4.7 below). The Warrant Holder will also ask the Search Target to set out the details of its privacy claim in writing to the CCPC's Director of Legal Services within 14 calendar days of the completion of the search operation, as provided for in paragraphs 5.1 to 5.3 below.

4.4. In some circumstances, the Search Target may be able, during the search operation, to identify specific electronic files or documents over which it wishes to make a claim of privacy. If the Warrant Holder considers that it would be practicable to consider such privacy claims at the search site, the Warrant Holder may examine such material – with the Search Target's consent – onsite to verify whether it is in fact private.

4.5. If the Warrant Holder accepts the privacy claim, he or she will direct the CCPC's onsite digital forensics authorised officer, or any other relevant authorised officer, not to seize or forensically copy such material. However, in circumstances where the Warrant Holder is not able to verify onsite that the material claimed to be private is in fact private, he or she will direct the CCPC's onsite digital forensics authorised officer (i) to proceed to seize the electronic device in question, or (ii) to forensically copy the relevant electronic material in accordance with the procedure set out below.

4.6. If the Warrant Holder directs the CCPC's onsite digital forensics authorised officer to forensically copy electronic material over which a privacy claim has been made by the Search Target, the CCPC's onsite digital forensics authorised officer will forensically copy and save such material onto a designated external storage device (the "Disputed Data Storage Device"). This Disputed Data Storage Device shall be used only for the storage of electronic material in respect of which a claim of privacy has been made by the Search Target. Electronic material in respect of which no privacy claim has been made by the Search Target will be stored on a separate external storage device or devices.

4.7. If the electronic material over which privacy has been claimed by the Search Target cannot be separated from other electronic material over which privacy has not been claimed – for example, where several emails within a single email account are claimed to be private while the rest are not – the entire file (e.g. a PST file) shall be forensically copied and saved onto the Disputed Data Storage Device by the CCPC's onsite digital forensics authorised officer, unless other methods of data sifting are available onsite which maintain the integrity of the electronic material in question.

4.8. Once all evidence has been collected from the search site by the CCPC authorised officers, the Disputed Data Storage Device will be logged by serial number and then sealed into an anti-static evidence bag by the CCPC's onsite digital forensics authorised officer. If any electronic device has been seized by CCPC authorised officers during the course of the search operation, such electronic device will also be logged by serial number and then sealed into an anti-static evidence bag by the CCPC's onsite digital forensics authorised officer. This authorised officer will then transfer the sealed evidence bags to the CCPC Site Exhibits Officer who will record the serial numbers of the sealed evidence bags on a chart listing all exhibits seized by the CCPC authorised officers at the search site (the "Site Exhibits Chart").

4.9. Thereafter, the sealed evidence bags will be transported back to the CCPC's offices by the Site Exhibits Officer where they will be handed over to the CCPC Case Exhibits Officer (i.e. a CCPC authorised officer who is responsible for all exhibits seized by the CCPC during all searches conducted in connection with that CCPC investigation). The CCPC Case Exhibits Officer will then transfer the sealed evidence bags to the CCPC's secure evidence room. The sealed evidence bags containing the Disputed Data Storage Device and any electronic device that has been seized by the CCPC during the search operation may be opened only by the CCPC's Digital Investigations Unit (following their retrieval from the secure evidence room – see paragraph 4.10 below).

4.10. All evidence gathered by CCPC authorised officers is stored in a secure evidence room at the CCPC's offices. In order to limit who has access to evidence stored in the evidence room, and thereby to maintain the security of such evidence, the evidence room is controlled by an access management system. Only a limited number of CCPC authorised officers have access to the evidence room ("Evidence Room Custodians"). Generally, evidence shall be transferred to the CCPC's Digital Investigations Unit and/or members of the CCPC case team by the relevant CCPC Case Exhibits Officer, who has obtained access to the evidence room via an Evidence Room Custodian.

C. Privacy claims raised in respect of hard copy material

4.11. If, during the course of a search operation, the Search Target claims that certain **hard copy items** (e.g. paper documents, folders, notebooks, etc.) should not be seized by the CCPC authorised officers because they contain private information, the Warrant Holder may examine such items – with the Search Target's consent – onsite to verify whether they are in fact private.

4.12. If the Warrant Holder accepts the privacy claim, he or she will direct the other CCPC authorised officers not to seize such items. However, in circumstances where the Warrant Holder is not able to verify onsite that an item claimed to be private is in fact private, or where material within an item over which privacy has been claimed by the Search Target cannot be separated from other material within that item over which privacy has not been claimed, the Warrant Holder will proceed to seize the entire item.

4.13. In these circumstances, the Warrant Holder will place the hard copy items over which privacy has been claimed into an envelope, which will be sealed, signed and transferred to the CCPC Site Exhibits Officer. The CCPC Site Exhibits Officer will record the serial number of the sealed envelope on the Site Exhibits Chart. Thereafter, the sealed envelope will be transported back to the CCPC's offices by the CCPC Site Exhibits Officer where it will be handed over to the CCPC Case

Exhibits Officer. The CCPC Case Exhibits Officer will transfer the sealed envelope to the CCPC's evidence room.

4.14. Depending on the circumstances, the CCPC may decide that the hard copy items contained in the sealed envelope should be converted into digital format. In such cases, the Case Exhibits Officer will transfer the sealed envelope from the CCPC's evidence room to an authorised officer from the CCPC's Digital Investigations Unit. The authorised officer from the CCPC's Digital Investigations Unit will then convert the hard copy items contained in the sealed envelope into digital format. At this stage, the digital version of the hard copy items will be accessible only by the CCPC's Digital Investigations Unit. The Digital Investigations Unit will deal with the digital version of those items in the same manner as electronic material over which privacy has been claimed by the Search Target (see Section 5 of the Protocol). The original hard copy items will be placed back into the envelope, sealed and returned to the CCPC Case Exhibits Officer, who will transfer the sealed envelope to the CCPC's evidence room.

D. Steps taken at the conclusion of the search operation

4.15. At the conclusion of the search operation, the CCPC authorised officer with responsibility for onsite digital forensics will prepare an inventory which describes the electronic material forensically copied (i.e. name of custodian, location from which the material was forensically copied and format of the material) and/or any electronic devices that have been seized by the CCPC authorised officers at the search site. The CCPC's onsite digital forensics authorised officer will provide a copy of the inventory to the Warrant Holder and/or the Site Exhibits Officer.

4.16. Before exiting the search site at the end of the search operation, the Warrant Holder will provide the Search Target with a copy of the Site Exhibits Chart. The Site Exhibits Chart will contain an inventory of all of the hard copy and electronic material seized/forensically copied by the CCPC authorised officers during the search.

5. VERIFIYING PRIVACY CLAIMS MADE BY A SEARCH TARGET

A. Making a detailed privacy claim to the CCPC

5.1. If the Search Target wishes, either during the search operation or after its completion, to make a claim that certain hard copy or electronic material seized or forensically copied by the CCPC during a search operation contains private information, the Search Target must set out the details of its privacy claim in writing to the CCPC's Director of Legal Services (as provided for in paragraphs 5.2 and 5.3 below) within 14 calendar days of the completion of the search operation. This must include all privacy claims made by the Search Target, whether they were initially made to the search team by the Search Target on the day of the search or are made subsequently. For the avoidance of any doubt, where the Search Target made a privacy claim during the search operation and such claim was accepted by the Warrant Holder on the day of the search (see paragraphs 4.4 and 4.5 above in respect of electronic material and paragraphs 4.11 and 4.12 above in respect of hard copy material), the Search Target is nevertheless required to confirm in writing the details of its privacy claim within 14 calendar days of the completion of the search operation. The 14-calendar day period referred to in this paragraph may be extended by the CCPC, at its absolute discretion, on the basis of a reasoned request from the Search Target.

5.2. When setting out the details of its privacy claim in correspondence to the CCPC's Director of Legal Services, the Search Target must identify the specific individual files or documents which the Search Target claims contain private information and provide reasons as to why each such file or document is considered to be private. In the case of electronic material, the CCPC considers that, in most cases, the details provided by the Search Target to the CCPC's Director of Legal Services should include:

a) the identity of the owner or custodian of the electronic material which is considered to contain private information;
b) the location or the specific device from which the files and/or documents considered to be private were forensically copied by the CCPC;
c) the name of each of the files and/or documents considered to be private; and
d) reasons as to why each such file or document is considered to be private.

5.3. In circumstances where CCPC authorised officers seized an entire electronic device during the search operation (e.g. a mobile phone, laptop, tablet etc.), the device will be brought back to the CCPC's offices, where the DIU Officer will make a forensic copy of the device. After this has been done, the CCPC will then return the device to the Search Target and, at the same time, will inform the Search Target in writing that it has 14 calendar days to notify the CCPC as to whether it wishes to make a privacy claim in respect of any items stored on the device. From the date of receipt of the device, the Search Target will have 14 calendar days within which to write to the CCPC's Director of Legal Services identifying the

specific items on the device in respect of which it wishes to make a claim of privacy (as provided for in paragraphs 5.1 and 5.2 above).

5.4. When the Director of Legal Services receives written correspondence from the Search Target in relation to the Search Target's privacy claim, a member of the CCPC's Legal Services Division will ask the CCPC Case Exhibits Officer to transfer the Disputed Data Storage Device from the CCPC's evidence room to an authorised officer from the Digital Investigations Unit (the "DIU Officer"). The DIU Officer is a shared resource who provides technical assistance in the context of the CCPC's enforcement activities and is not generally directly involved in the conduct of the CCPC's investigation.

5.5. If the CCPC's Director of Legal Services does not receive any correspondence from the Search Target in relation to the Search Target's privacy claim within 14 calendar days of the completion of the search operation, or – where an entire electronic device was seized during the search operation – within 14 calendar days of such device being returned to the Search Target, the DIU Officer will proceed to release to the CCPC case team all electronic material and electronic devices seized or forensically copied from the search site, with the exception of any material over which a claim of legal professional privilege has been made. In such cases, the CCPC case team will also have access to all hard copy material seized during the search operation, with the exception of any material over which a claim of legal professional privilege has been made.

B. Initial processing of electronic material claimed as private

5.6. The CCPC has developed the process set out in the paragraphs below for the processing of electronic material claimed by the Search Target to be private. Whilst the CCPC considers the following process to be appropriate to most cases, it may depart from such process as a matter of its sole discretion in appropriate cases.

5.7. The Disputed Data Storage Device will be unsealed by the DIU Officer within the CCPC's 'Forensic Laboratory'. The CCPC's Forensic Laboratory is comprised of physically isolated and protected hardware located in an access-secured area in the CCPC's offices. The forensic workstations in the CCPC's Forensic Laboratory are not connected to the CCPC's network but instead have access to a segregated dedicated network for use of forensic analysis with no access to public networks. Access to the CCPC's Forensic Laboratory is restricted to staff members of the CCPC's Digital Investigations Unit and a small selection of high level management within the CCPC. Access to systems in the CCPC's Forensic Laboratory is restricted to staff members of the Digital Investigations Unit only.

5.8. The DIU Officer will forensically copy the electronic material in respect of which a privacy claim has been made by the Search Target from the Disputed Data Storage

Device using a forensic workstation in the Forensic Laboratory. The copied electronic material will be scanned for malware and any viruses before being transferred to the CCPC's eDiscovery server, where it will be stored at a location separate from other electronic material relating to the CCPC's investigation. At this stage, it will be accessible only by the CCPC's Digital Investigations Unit.

5.9. The DIU Officer will then create a separate "case" within the CCPC's eDiscovery platform, which will be labelled with the name of the CCPC's investigation and will also be labelled 'Disputed Data Restricted'. This "case" will be accessible only from within the CCPC's Forensic Laboratory and will be available only to staff of the Digital Investigations Unit.

5.10. The DIU Officer will then upload the copied electronic material to the 'Disputed Data Restricted' case on the eDiscovery platform. The DIU Officer will produce a report which records any processing errors. Processing errors include but are not limited to:

a) corrupt data;
b) failure to decrypt data;
c) unknown file types;
d) excessively large data;
e) empty files.

5.11. To the extent possible, the DIU Officer will try to resolve any processing errors by investigating the affected material from a top level (i.e. without looking into the contents of any individual file or document). Where it is not possible to do so, any remaining processing errors will be referred by the DIU Officer to the CCPC's Legal Services Division and to the case manager within the CCPC case team for instructions on how to proceed.

5.12. Once all processing issues have been resolved, the electronic material will be processed into the eDiscovery platform by the DIU Officer. An index listing all of the metadata relating to the electronic material (the "Index") will be generated by the DIU Officer and will be exported from the eDiscovery server onto a USB device. The Index will contain all of the metadata for each individual file or document, including the document name, size, extension, date of creation, date on which it was modified, etc. The metadata contained in the Index will not include any information about the contents of an individual file or document. For the avoidance of any doubt, the DIU Officer will not look at the contents of any individual file or document during the creation of the Index.

5.13. A unique hash value and a unique CCPC eDiscovery index number will be allocated to each individual file or document which has been processed into the eDiscovery platform. The hash value and CCPC eDiscovery index number allocated to each individual file or document will be included in the Index generated by the DIU Officer to allow the precise identification of individual files or documents which

the Search Target claims contain private information. The hash values of the files and documents processed into the eDiscovery platform remain constant throughout the process described in this Section and can be traced back to the original electronic material that was forensically copied by the CCPC during the search operation.

5.14. The DIU Officer will deliver the Index to the Privacy Review Team (as referred to in paragraph 5.15 below). The Disputed Data Storage Device will be returned by the DIU Officer to the CCPC Case Exhibits Officer in a new sealed and labelled bag. The CCPC Case Exhibits Officer will return it to the CCPC's evidence room.

C. Verifying privacy claims made in respect of electronic material

Role of the Privacy Review Team

5.15. In order to deal with privacy claims made by the Search Target, the CCPC's Director of Legal Services will appoint a private data review team (the "Privacy Review Team") which will normally consist of an authorised officer from the CCPC's Digital Investigations Unit and a representative from the CCPC's Legal Services Division, both of whom will, where possible, have no direct involvement in the CCPC's investigation.

5.16. The Privacy Review Team will conduct a review of the electronic material which is claimed by the Search Target to contain private information for the purpose of reaching a view as to whether or not such material contains private information. In order to do so, the Privacy Review Team will review each file or document which the Search Target claims contains private information and will consider the details of the privacy claim set out in writing by the Search Target. The process that will be followed by the Privacy Review Team is set out in paragraphs 5.19 to 5.27 below.

5.17. After completing its review of the electronic material claimed to be private by the Search Target, the Privacy Review Team may decide that some of the material appears to contain private information but is nonetheless potentially relevant to the CCPC's investigation. In such cases, the Privacy Review Team may reject the Search Target's privacy claim in respect of such material. As a matter of principle, the CCPC considers that the CCPC case team is entitled to review, and use in its investigation, any files or documents which the Privacy Review Team has decided are potentially relevant to the CCPC's investigation even if the Search Target has claimed that the files or documents in question contain private information. For example, email correspondence between a husband and wife about being late home due to a meeting, which is claimed by the Search Target to be private, may nonetheless be potentially relevant to the CCPC's investigation if it transpires that the meeting referred to in that correspondence took place at the same time and location as a meeting which is alleged to have taken place between participants in the suspected anti-competitive conduct being investigated by the CCPC.

5.18. Therefore, during the course of its examination of the Search Target's privacy claims, the Privacy Review Team will consider whether the material in question is potentially relevant to the CCPC's investigation. As part of this exercise, the Privacy Review Team may apply to each of the files and/or documents claimed to be private any keywords and search parameters used by the search team during the course of the search operation for the purpose of identifying potentially relevant material and/or any keywords and search parameters developed by the CCPC case team following the completion of the search operation. If this generates any 'hits', the Privacy Review Team will look at the results of the keyword searches to see whether any of the files or documents appear to be potentially relevant to the CCPC's investigation.

Process adopted by the Privacy Review Team

5.19. When the Director of Legal Services receives correspondence from the Search Target which identifies the particular files and/or documents which the Search Target considers contain private information, the Legal Services Division will provide this information to the Privacy Review Team. The Privacy Review Team will ask the DIU Officer to extract from the 'Disputed Data Restricted' case in the eDiscovery platform the files and/or documents which are claimed by the Search Target to contain private information. The Privacy Review Team will then examine each of those files and/or documents in order to verify whether they contain private information.

5.20. Where a file or document contains some business-related information intermingled with private information, the Privacy Review Team will examine the entire file or document in question. The Privacy Review Team will examine the files and documents identified by the Search Target for no longer than is necessary to reach a view as to whether or not they contain private information.

5.21. Following its examination of the Search Target's privacy claims, the Privacy Review Team will inform the Director of the Legal Services Division as to its findings for each file or document in respect of which privacy has been claimed by the Search Target i.e. whether the Privacy Review Team:

a) agrees with the Search Target's claim that a file or document contains private information and has concluded that the file or document does not appear to be relevant to the CCPC's investigation;
b) disagrees with the Search Target's claim that a file or document contains private information; or
c) rejects the Search Target's claim on the basis that the Privacy Review Team considers that a file or document appears to contain material which is private but which is nonetheless potentially relevant to the CCPC's investigation.

5.22. The Legal Services Division will then inform, in writing, the Search Target of the outcome (with reasons) of the Privacy Review Team's examination of the Search Target's privacy claims.

5.23. Where the Privacy Review Team disagrees with the Search Target's claim that a file or document contains private information (paragraph 5.21(b) above) or considers that a file or document which is claimed to be private contains material which is potentially relevant to the CCPC's investigation (paragraph 5.21(c) above), the Legal Services Division will inform the Search Target that it has 14 calendar days to object to the Privacy Review Team's findings. If no objection to the Privacy Review Team's findings is received from the Search Target within 14 calendar days of being informed of those findings by the Legal Services Division, the files and documents referred to in paragraph 5.21(b) and/or paragraph 5.21(c) will be made available to the CCPC case team.

5.24. If the Search Target submits a reasoned objection to the Privacy Review Team's findings within 14 calendar days of being informed of those findings by the Legal Services Division, the Privacy Review Team will review the file(s) and/or document(s) in question for a second time in light of the Search Target's objections.

5.25. If, having conducted a second review of the relevant file(s) and/or document(s), the Privacy Review Team considers that the file(s) and/or document(s) in question do not contain private information (or that, while containing private information, are nonetheless relevant to the CCPC's investigation), the Privacy Review Team will inform the Legal Services Division as to its final decision. The Legal Services Division will then inform, in writing, the Search Target of the Privacy Review Team's final decision and the reasons for the decision.

5.26. If the Search Target disagrees with the Privacy Review Team's final decision, it is a matter for the Search Target to decide whether or not it wishes to bring a legal challenge against the Privacy Review Team's final decision. If, within 7 calendar days of being informed of the Privacy Review Team's final decision by the Legal Services Division, the Search Target informs the Legal Services Division, in writing, that it intends to institute legal proceedings against the Privacy Review Team's final decision, the files and documents referred to in paragraph 5.21(b) and/or paragraph 5.21(c) will not be released to the CCPC case team pending the resolution of the matter. If, however, the Search Target does not institute proceedings by making an application to the relevant court within 14 calendar days of the date of the Search Target's written notification to the Legal Services Division that it intends to institute legal proceedings, the files and documents referred to in paragraph 5.21(b) and/or paragraph 5.21(c) will be made available to the CCPC case team. Similarly, if, within 7 calendar days of being informed of the Privacy Review Team's final decision by the Legal Services Division, the Search Target has not informed the Legal Services Division, in writing, that it intends to institute legal proceedings against the Privacy Review Team's final decision, the files and documents referred to in paragraph 5.21(b) and/or paragraph 5.21(c) will be made available to the CCPC case team.

5.27. If the Privacy Review Team agrees with the Search Target's claim that a file or document contains private information and has concluded that the file or

document is not relevant to the CCPC's investigation, the CCPC will follow the process described in the paragraphs below.

D. Processing electronic material verified as private

5.28. Where the Privacy Review Team agrees with the Search Target's claim that a particular file or document contains private information and decides it is not relevant to the CCPC's investigation (paragraph 5.27 above), the DIU Officer will use the hash values and CCPC eDiscovery index numbers to identify each such file or document in the 'Disputed Data Restricted' case in the eDiscovery platform. The DIU Officer will then label each such file or document in the 'Disputed Data Restricted' case in the eDiscovery platform with a 'Private Data' tag to ensure that it will be excluded from the data set which will be made available to the CCPC case team for their review.

5.29. All files and documents that are not marked with a "Private Data" tag will be exported by the DIU Officer from the 'Disputed Data Restricted' case and will be added to the data cache of the review case in the eDiscovery platform (which is accessible by the CCPC case team). The review case will be taken offline from the CCPC case team during this process and will be available only to the DIU Officer at this stage.

5.30. Before the review case is made available to the CCPC case team, the DIU Officer will search the review case for any of the hash values allocated to files or documents which have been verified by the Privacy Review Team as containing private information. If any such files or documents are identified, the DIU Officer will ensure that those files and/or documents will be hidden from the CCPC case team on the eDiscovery platform by restricting access to such files and/or documents.

5.31. The DIU Officer will then release the review case back to the CCPC case team so that they can continue their review of the electronic material on the eDiscovery platform.

5.32. At any stage in the process, the DIU Officer can generate a report which will identify who had access to particular files or documents on the 'Disputed Data Restricted' case on the eDiscovery platform, from which location the files or documents were accessed and any actions performed on the files or documents (e.g. opening of files).

5.33. The 'Disputed Data Restricted' case on the eDiscovery platform will remain active but may be accessed only by the DIU Officer while the CCPC's investigation or any resulting legal proceedings are ongoing. Deletion of the electronic material contained on the 'Disputed Data Restricted' case on the eDiscovery platform will not occur until after the CCPC's investigation has been closed, or after a final judgment in any resulting legal proceedings has been obtained, so as to ensure that the integrity of the electronic material is maintained.

5.34. In certain exceptional cases, subsequent to a decision by the Privacy Review Team that certain electronic material contains private information and is not relevant to the CCPC's investigation (and where the electronic material in question has therefore not been made accessible to the CCPC case team on the eDiscovery platform), the CCPC case team may form the view or come into possession of information indicating that (i) such material does not, in fact, contain private information or that (ii) such material appears to contain private information but is nonetheless relevant to the CCPC's investigation. If the CCPC considers that a re-examination of certain electronic material is justified on the basis of the CCPC case team's views, it may instruct the Privacy Review Team to re-examine the electronic material in question in order to determine whether it contains private information and whether any private information is nonetheless relevant to the CCPC's investigation. If the CCPC decides to instruct the Privacy Review Team to re-examine the electronic material in question, it will inform the Search Target of the fact that it has decided to do so and will give the Search Target reasons for its decision. For the avoidance of any doubt, the process followed thereafter will be the same as the process set out in paragraphs 5.20 to 5.33 above.

E. Dealing with privacy claims in respect of hard copy material

5.35. In the case of hard copy items which have been seized by the CCPC and in respect of which a privacy claim has been raised by the Search Target, where the CCPC has decided to convert the relevant hard copy item into digital format (as provided for in paragraph 4.14 above) the privacy claim will be assessed by the CCPC on the basis of the process set out in Sections 5.B to 5.D above. Where the Privacy Review Team agrees with the Search Target's claim that a particular hard copy item contains private information (paragraph 5.21(a) above), the CCPC will return the original item to the Search Target.

5.36. In the case of any seized hard copy item in respect of which a privacy claim has been raised by the Search Target and where the CCPC has decided <u>not</u> to convert the relevant hard copy item into digital format, the item in question will be reviewed by the Privacy Review Team. The Privacy Review Team will examine the item for no longer than is necessary to reach a view as to whether or not it contains private information. Where the Privacy Review Team considers that certain material within the item is private but that other material within that item is not private (see paragraph 4.12 above), the Privacy Review Team will ask the CCPC's Digital Investigations Unit to convert the item in question into digital format. After this has been done, the Digital Investigations Unit will provide a copy of the digital version of the item to the Privacy Review Team. At this stage, the digital version of the item will be accessible only by the CCPC's Digital Investigations Unit and the Privacy Review Team. The Privacy Review Team and the Digital Investigations Unit will ensure that any material considered by the Privacy Review Team to be private will be redacted from the digital version of the item. The original hard copy item will not be changed by this process and will be accessible only by the CCPC's Digital Investigations Unit and the Privacy Review Team at all times during this process.

5.37. Thereafter, the process set out in paragraphs 5.21 to 5.26 will be applicable. Where the Privacy Review Team agrees with the Search Target's claim that a particular hard copy item contains private information and has concluded that the item is not relevant to the CCPC's investigation (paragraph 5.27 above), the CCPC will return the original item to the Search Target.

6. CLAIMS THAT MATERIAL SEIZED DURING A SEARCH OPERATION IS NOT RELEVANT TO THE INVESTIGATION

6.1. For the avoidance of doubt, the process described above in Sections 4 and 5 of the Protocol relates only to claims that the CCPC has seized or forensically copied private information; it does not cover claims that the CCPC has seized or forensically copied material that is not relevant to the CCPC's investigation. The CCPC considers that relevance is a matter to be determined by the CCPC case team, and not the Search Target, as the CCPC's investigation progresses.

6.2. As outlined above in Sections 2 and 4 of the Protocol, there are various safeguards in place, both before and during the conduct of an unannounced search, which aim to ensure that the search team is focused on identifying and forensically copying or seizing material that is potentially relevant to the CCPC's investigation. In particular, these safeguards include but are not limited to:

a) the CCPC takes a decision to deploy its powers under section 36 or 37 of the 2014 Act in a particular investigation only after considering all of the investigation tools available to the CCPC and concluding that a search under section 36 or 37 is the most appropriate investigation tool for uncovering, at an identified business premises or private dwelling, information which may be required in relation to the matter being investigated by the CCPC;
b) the requirements under section 36(4) and 37(3) of the 2014 Act to satisfy a judge of the District Court that there are reasonable grounds for suspecting that evidence of, or relating to, the commission of an offence is to be found in the identified business premises or private dwelling;
c) the CCPC conducts research in the lead up to the search operation for the purpose of identifying persons of interest and the devices, locations and custodians which may hold material that is potentially relevant to the CCPC's investigation;
d) the search team and the Digital Investigations Unit generally meet periodically in advance of the search operation for the purpose of ensuring that all CCPC authorised officers involved in the search are fully prepared and can search the identified business premises or private dwelling in a targeted way;
e) the CCPC provides the Search Target with a copy of the search warrant and an explanatory note describing the purpose of the search at an early stage in the search operation;
f) the search team focuses the search on custodians, devices, offices, etc. identified in advance by the search team;
g) CCPC authorised officers use keywords and other search parameters to identify material that is potentially relevant to the CCPC's investigation both during the search operation and during the subsequent review of seized and forensically copied material at the CCPC's offices.

6.3. If the Search Target has concerns that material seized or forensically copied by the CCPC during a search operation is not relevant to the CCPC's investigation, the Search Target should set out the details of its concerns in writing to the CCPC case team. The CCPC case team may take those concerns into account. However, the CCPC considers that, ultimately, it is a matter for the CCPC case team to decide whether or not material is potentially relevant to the CCPC's investigation.

6.4. In many cases, a cursory review of an individual file or document will not be sufficient for the CCPC to reach a definitive view as to whether or not that file or document is relevant to its investigation. In these circumstances, if the CCPC considers that an individual file or document is potentially relevant to its investigation, it may take steps to seize or forensically copy that file or document (unless it is material over which a claim of legal professional privilege or privacy has been made by the Search Target and verified by the CCPC – see Sections 4 and 5 of the Protocol). The CCPC may be able to make a definitive decision as to the relevance to the CCPC's investigation of certain material only at a much later stage in the CCPC's investigation. It may only be as a result of careful and detailed cross-referencing by the CCPC case team of all of the material that was forensically copied and seized during a search operation that the CCPC case team reaches a view that an individual file or document constitutes evidence of the suspected anti-competitive conduct. Until that point, the file or document in question remains potentially relevant to the CCPC's investigation. For this reason, the CCPC considers that the CCPC case team is best placed to determine whether material is potentially relevant to the CCPC's investigation.

6.5. It is also worth noting that the CCPC case team's views as to whether an individual file is potentially relevant to the CCPC's investigation may evolve over time based on the CCPC case team's understanding of the facts of the case and of the suspected anti-competitive conduct being investigated. For example, as its investigation progresses, the CCPC case team may develop new keywords and search parameters for the purpose of identifying potentially relevant material which generate 'hits' in files or documents which have not up to that point been reviewed in detail by the CCPC case team.

6.6. If, during the course of the CCPC's investigation, the CCPC case team ultimately decides that certain material that was forensically copied or seized during a search operation is not relevant to the CCPC's investigation, the CCPC will take steps to ensure that such material is put beyond the access of the CCPC case team. In the case of hard copy items, this may involve taking steps to return to the Search Target the original hard copy item which was seized by CCPC authorised officers during the search operation. In the case of electronic material, this may involve taking steps to ensure that such material will be hidden from the CCPC case team on the eDiscovery platform by restricting access to such material and will be accessible only by the CCPC's Digital Investigations Unit while the CCPC's investigation or any resulting legal proceedings are ongoing. Deletion of electronic material which is determined by the CCPC to be not relevant to the CCPC's investigation will not occur until after the CCPC's investigation has been closed, or after a final judgment in any resulting legal proceedings has been

obtained, so as to ensure, firstly, that the integrity of the electronic material is maintained and, secondly, that inculpatory and exculpatory material is retained and remains available for the duration of the CCPC's investigation and any resulting legal proceedings.

7. SAFEGUARDS IN RESPECT OF CONFIDENTIAL INFORMATION AND PERSONAL DATA

A. Protection of confidential information

7.1. The CCPC is committed to taking all necessary steps to protect commercially sensitive and confidential information obtained by the CCPC in the performance of its functions (including information seized or forensically copied by the CCPC during a search operation conducted under section 36 or 37 of the 2014 Act) at all stages of its investigations.

7.2. Section 25(1)(a) of the 2014 Act contains a prohibition on the unauthorised disclosure by any person of confidential information obtained by him or her in his or her capacity, or while performing duties as, a Member of the CCPC, a member of staff of the CCPC, an authorised officer of the CCPC or a person engaged by the CCPC in any other capacity. The CCPC may disclose commercially sensitive and/or confidential information obtained by the CCPC in the performance of its functions only if such disclosure would be in accordance with section 24 or section 25 of the 2014 Act or if such disclosure is required by or is in accordance with other applicable provisions of Irish or European law. The CCPC considers that it has the right to disclose such material to its external advisors as it deems appropriate, and to disclose material for the purpose of court proceedings, which may include material obtained by the CCPC through the use of its statutory powers.

7.3. All material obtained by the CCPC from parties to investigations is stored in the CCPC's evidence room. Within the evidence room, all material relating to a particular investigation is kept within the same cabinet(s) which is at all times securely locked and is accessible only by the relevant CCPC Case Exhibits Officer (i.e. the Case Exhibits Officer appointed in respect of the CCPC investigation in question) and an Evidence Room Custodian. In relation to electronic material obtained by the CCPC from parties to investigations, once the electronic material has been uploaded to the CCPC's eDiscovery platform by the CCPC's Digital Investigations Unit, access to such material via the eDiscovery platform is restricted to members of the CCPC case team which have been assigned to the CCPC investigation in question. The CCPC adopts various safeguards to ensure that confidential information contained in material (whether in hard copy or electronic format) which has been obtained from one party to an investigation is not disclosed to other parties to the investigation.

B. Compliance with data protection law

7.4. The CCPC is committed to respecting the privacy of individuals and to complying with applicable data protection laws, including the EU General Data Protection Regulation (i.e. Regulation (EU) 2016/679), the Law Enforcement Directive (i.e. Directive (EU) 2016/680) and the Data Protection Acts 1988 to 2018.

7.5. The CCPC – in its capacity as a data controller – has various obligations under data protection law with respect to the processing of personal data. Information on the manner in which the CCPC processes personal data is outlined in the privacy notices published on the CCPC's website: https://www.ccpc.ie/business/privacy/.

7.6. For the purpose of this Protocol, the CCPC acknowledges that material obtained by the CCPC in the performance of its functions (including material seized or forensically copied by the CCPC during a search operation conducted under section 36 or 37 of the 2014 Act) may contain "personal data" (as defined in the EU General Data Protection Regulation). Subject to and in accordance with applicable law, the CCPC will ensure that the processing by the CCPC of any personal data contained in such material is compliant with the CCPC's obligations under data protection law. In particular, the CCPC will not keep personal data for longer than is necessary for the purpose or purposes for which it was obtained. In practice, this means that after the closure of a CCPC investigation, or after a final judgment in any resulting legal proceedings has been obtained, the CCPC will consider whether electronic material relating to the investigation in question may be deleted or, in the case of hard copy items, whether steps should be taken with a view to returning to the Search Target any original hard copy items seized by CCPC authorised officers during the search operation.