USER TERMS

Valid from: 01.11.19

By applying to register online as a user ("a User" or "Users") you agree to the following terms and conditions and enter into an agreement with DisputesEfiling.com Limited (DEF, the Provider) which take effect the moment you begin making your application to register for access to the DEF Platform ("the Platform", "the System" or "the Service").

Administration matters

Database Administrator

The Platform is managed by the Database Administrator. The Database Administrator can be contacted via Support; please follow the link (coloured red) in the top right hand corner on every page of the Platform.

By registering online and accepting these User Terms you are consenting to the Database Administrator having access to your cases. Such access is strictly limited to:

a) Enabling DEF to respond to Users about the technical performance of the Platform; and,
b) Any other queries of a technical nature only.

Such access is, we are sure you understand, essential for the smooth running of the Platform and to the benefit of all Users.

The Database Administrator is unable to address any issues of substantive law or issues arising from the conduct of any particular case.

Scheme and other Administrators/Registrars

Individual ADR schemes are managed by their own Administrators/Registrars. In the event of any queries concerning the running of the schemes themselves please contact the Scheme Administrator concerned.

Administrators are also necessary for solicitor law firms, defence organisations, departments of in house Counsel and similar. Any queries regarding validation of individual users (or other issues) within such organisations should be addressed to the Administrator in question, NOT the Database Administrator.

By registering online and accepting these User Terms you are consenting to the Scheme and other Administrators/Registrars having access to your cases. Such access is strictly limited to:

a) Enabling Scheme and other Administrators/Registrars to respond to Users about issues relating to their Schemes; and,
b) Undertaking supervision and/or compliance actions necessary for the lawful operation of their Schemes.

Such access is, we are sure you understand, essential for the smooth running of the Schemes and to the benefit of all Users.

The Scheme and other Administrators/Registrars are unable to address any issues of substantive law or issues arising from the conduct of any particular case.

1. Registering as a User of the System

To use the System you will need to register through oneplatform.disputesefiling.com providing accurate details on the registration page, creating a User name and password, agreeing to these terms and confirming your email address. You then become a "User" of the system.

Please keep your User name and password secret.

2. Provision of service and fees

On registration as a User you pay nothing.

A commencement fee is payable in order to use each of the services available on the Platform on a per party basis except for arbitrations in the PIcArbs Scheme which are charged per case. This means that a separate fee is payable for each party to a case and for each service. A fee will be charged in the event one form of ADR is converted to another form of ADR on the Platform (the "Convert" function).

The following examples illustrate the charging arrangements:

For each party the fee is £62.50 plus VAT. In the usual situation where there is one Claimant and one Defendant the total fee is therefore £125 plus VAT. For every additional party the fee is a further £62.50 plus VAT. The invoice will charge a single fee being calculated as the aggregate of the fee for each party added.

Here are some illustrative examples of how our invoicing works:

Opening a pre-action case – a fee is charged

If pre-action is converted to arbitration – a fee is charged

If arbitration is converted to mediation – a fee is charged

If that mediation is converted back to arbitration – no fee is charged as a fee was already charged for opening that arbitration case

If a C-ADR case is opened to resolve any costs issues – a fee is charged.

Starting a pre-action case

On commencing a pre-action case the commencing User incurs a fee payable to DEF. This covers:

(a) registration of you and/or your organisation as a party to pre-action activity;
(b) registration of the opposing party/ies and/or their solicitor and his/her/their firm; and,
(c) opening of the individual case to commence pre-action work.

Starting ADR (arbitration, mediation, adjudication, Construction Adjudication or evaluation) via any Provider

On commencing ADR on the Platform payment of the Commencement Fee covers:

(a) registration of you and/or your organisation as a party a party's representative in the ADR process;
(b) registration of the opposing party/ies and/or their representatives;

(c) registration of Insurer or other Indemnifier e.g. AXA or NHS Resolution;
(d) registration/appointment of the Neutral or Neutrals; and,
(e) opening an e-file through which to commence and manage the relevant ADR process;

3. After commencement the Provider will enable each User to access the System throughout the case.

You as a User agree with DEF as follows:

4. Rules

(1) To abide by the terms, rules and codes of practice incorporated into any relevant agreement entered into prior to the instruction of an organisation providing adjudication, Construction Adjudication, neutral evaluation, mediation and/or arbitration services (ADR).

Invoices and payments

(2) An invoice for the relevant fees together with VAT at the prevailing rate will be sent electronically to the party responsible for the payment of fees on a case being opened, i.e. when clicking: "submit case". In the case of litigants in person this will be to the individual litigant. In the case of Schemes or Firms the invoice will be sent to the relevant nominated Administrator to arrange payment. Payment must be made by bank transfer to the bank account details of which are on the invoice.

(3) To pay (by bank transfer) the relevant fees in the invoice on receipt of that invoice for opening a pre-action case or starting an evaluation, mediation or arbitration in accordance with the terms of payment set out in these user terms or as varied by separate agreement.

Failure to pay fees

(4) If any User fails to pay any fees then access to the case in question will be denied. Interest may be charged on the late payment of such fees at 10% above the Bank of England base rate. Further, until the relevant fee is paid the user will not be able to access the case in question.

Permitting access

(5) Accurately and carefully to complete the relevant online form so as to ensure that you permit the parties' representatives and other authorised users involved in the case proper access to the System by provision of correct email addresses.

EFiling

(6) To file all relevant documents in the System through the e-filing system and NOT to send them by email whether as attachments or otherwise.

Software integrity

(7) Not to nor to attempt to copy or emulate the System or software in whole or in part and not to cause any third party to do so.

Professional communication

(8) Not to send any illegal, insulting, abusive or rude communication through any of the e-filing services and never to use these services for private communications. The Service is for the conduct of civil claims and services associated with that process. If such communications are sent then The Provider reserves the right to terminate access by the User in question.

Viruses

(9) To bear responsibility for the virus free condition of the documents which you upload. The System shall not bear any liability whatsoever if a User uploads a document which is infected with a virus or damaged macro or other damaging content and that document is then downloaded by another User and causes damage to that other User. The System is a case and hearing management system not a filtering system.

Communication with and/or from the Database Administrator

(10) To permit the System's Database Administrator to contact Users to keep them up to date with changes to the user terms, procedures, charges and to effect service of all notices sent under these user terms to the User's registered e-mail address. Further to permit communications to Users to advise about System critical alerts or to advise about occasions when routine maintenance is due to take place.

Tampering

(11) Not to alter the registered User details of any other party or any solicitor, counsel, Evaluator, Mediator or Arbitrator or other User with access to any individual case on the System, unless permitted by that person.

Service

(12) Insofar as service of any document is required, service takes place when a User uploads a document onto the System and that User is given permission to view the document being served.

Spam & Virus filters

(13) Ensure that emails from the Service are allowed by the User's spam and virus filters. Please read our FAQs for further information on whitelisting etc.

Non receipt of emails

(14) Accept that email notification to the User of an e-filing/document viewing permission being granted will be sent by the System to the User's registered email address and the User agrees that receipt takes place when the email is sent to that User and that notification by email from the System has been sent to the User's registered email address whether it is received there or not. DEF retains a log of all sent email notifications.

Security

(15) not to leave the e-filing platform open on the User's computer whilst the User leaves his or her desk for any period of time, but instead to log off immediately before leaving the computer. In the event there is no keystroke for 30 minutes the system will automatically log-off any User. Users must follow the Security requirements set out in para 11 of these User Terms, below.

Type of Documents you can file

(16) The System caters for the following formats:

Word (DOC and DOCX), PDF, Excel (XLS and XLSX), JPEG (JPG) and the following video formats: AVI, MOV and MP4

Please ensure you only upload documents and image/video files in such formats.

Data processing consent

(17) By using the System you understand, consent to and accept that:

DEF and any of the providers of services on the Platform are permitted to hold and process the data in the System and the data entered onto the System by you as a User and the data entered in the "fill in" forms on the System, limited to the following data for the parties, their lawyers and/or insurers or others:

i) names and addresses;
ii) telephone numbers;
iii) email addresses;
iv) the start date of the claim;
v) the type of claim made;
vi) claim values;
vii) dates of settlement agreements;
viii) date of the end of each case;
ix) settlement sums involved; and,
x) the start to end cycle times.

The System processes data in civil litigation, ADR and pre-action activity in reliance on the further grounds set out in Article 6.1 GDPR as follows:

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party

In relation to our reliance on ground 6.1(b) we confirm compliance with the requirements explained in the EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, dated 8 October 2019.

In the event the UK leaves the EU without an agreement as to the transfer of data the Appendix to these User Terms will apply in addition to the above grounds for data processing and international transfers. The Standard Contractual Clauses set out in the Appendix will in those circumstances form part of the agreement created when Users accept these User Terms.

(18) The System will store all of the parties' e-filed documents some containing specific, identifiable health data and data relating to children. The System will not use or process (other than storing) the information in these documents in any way beyond e-storage for the relevant services provided by the Platform. The Platform relies on the exception at Article 9.2(f) GDPR to process such data namely: processing is necessary for the establishment, exercise or defence of legal claims.

(19) No personal, identifiable data will be shared by the System with any person other than those registered as Users unless the law requires the System to deliver up such data to prosecuting authorities or Government and DEF and the other providers have no legal right to refuse.

(20) Anonymised data may be shared by DEF with law firms and other institutions from time to time under commercial terms entered into by DEF with those third party organisations. No such data will

contain any personal details and is shared in permanently anonymised form only for the purpose of statistical analysis, performance reviews, trend reviews and the like.

(21) The System may store data for up to 7 years after the date of the conclusion of a case if that data could be relevant to any breach of contract claim which may be made against the Provider by any User.

(22) For the contact details of the data protection officer for each of the services on the Platform please consult the information web sites of each service.

(23) The Data Protection Officer for the Platform is contactable via tonyguise@disputesefiling.com. Our privacy notice is available here: https://www.disputesefiling.com/privacy-notice.php

(24) All Users agree that the System may store User's data on the Provider's servers based in England until such time as such data is deleted as provided by paragraph 9 of these User Terms and DEF's Data Retention and Disposal Policy.

(25) International Transfers of Personal Data

Considering the global reach of DEF's business, your Personal Data may be downloaded in the Americas, EMEA and Asia-Pacific regions, including locations where data privacy legislation may differ from that in your country.

DEF has in place appropriate measures to ensure the validity of Personal Data transfers to countries in which there may not be a similar level of protection as in your country and as required under applicable data protection and privacy laws. Those measures are described in detail below and take advantage of permitted derogations from the prohibition against international transfers contained within the EU's GDPR.

Pursuant to Articles 44, 45-47 and 49 of the GDPR you agree that where relevant for your case we may transfer personal data to a Third Country. That is to say to a country that is not a country of the European Economic Area as defined for the purposes of the GDPR.

(26) Where there are no Adequacy Decisions or Binding Corporate Rules to make such transfers lawful then DEF relies on the derogations which are permitted (as set out in Article 49) from the prohibition of such International Transfers in Article 44.

(27) The derogations in Article 49 upon which DEF relies are:

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request

or:

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person

or:

(e) the transfer is necessary for the establishment, exercise or defence of legal claims.

Transfers of personal data to the USA take place in the context of the Adequacy Decision in relation to the USA which is restricted to those entities who/which have certified compliance with the EU-US Privacy Shield of 2016. To the extent a recipient of personal data is not certified compliant with the EU-US Privacy Shield then DEF relies on the grounds set out in rule 27 of paragraph 4, above.

5. The e-file

In consideration of the User paying the relevant fee the System will register his or her details as a User and create a case number and an individual e-file for each service purchased.

Uploads can be a maximum of 500MB for any one upload with a maximum capacity for each case of 5GB. A fair dealing policy applies to upload sizes and case capacity. This is subject to review in the event of uploads or cases regularly in excess of these limits.

6. The purpose of the System

The e-filing system is provided by DEF to assist Users in each case. In accordance with this requirement all Users must only use the Platform for communicating about and exchanging documents in any case being managed on the Platform. This is to ensure that Users' data is protected in accordance with these Terms.

7. Availability of service

The Provider will make all reasonable efforts to ensure that the e-filing software is fully functioning during business hours (08.00 and 18.00 GMT) 5 days per week (and out of normal working hours too, if possible) save when the:

(i) System's storage provider's facilities are interrupted;

(ii) System's storage provider's internet facilities are interrupted;

(iii) Power is cut in any link in the chain necessary to provide the online service;

(iv) Government or terrorist action prevents the provision of the Service; and,

(v) The Platform is being upgraded, repaired or maintained which will usually occur during weekends or overnight between 18.00 and 09.00 on any day of the week but may overrun into working hours.

8. Warranty and permission to store and warranty

8. Users:

(i) Permit and require the Provider to store the documents which are filed for the duration of the individual case and any subsequent costs related alternative dispute resolution process; and,

(ii) Warrant that the User has all necessary permissions from the party which he/she represents to e-file all documents or from whoever needs to provide permission.

9. Destruction of EFile

Subject to the provisions of rule 21 in paragraph 4 above, the Provider will be entitled to destroy the e-file without further notice following the expiry of 90 days after the closure of the case. Further details of the process and applicable standards are provided in our Data Retention and Disposal Policy, available on request. This process does not apply if Users have agreed to use ADR for resolving any costs disputes in a case and have commenced a costs related ADR process via the C-ADR online module on the Platform, in which case the file will be maintained until 90 days after the costs are settled or finally determined whichever is sooner.

10. Back-up copies

The User must keep electronic "back up" copies of all documents which Users have filed through the System and of all documents which have been filed or served by any other User in all individual cases in which Users are involved.

11. Security

The Provider will make all reasonable efforts to ensure that the e-filing system is as secure as reasonable industry standards require. Further details about the data security measures employed are available in our Data Security Statement which is available at https://www.disputesefiling.com/data-security.php

12. The Provider shall not be liable for any damages or costs if Users' name and password are hacked, stolen, or used by another malicious person and in some way an e-file is interfered with. DEF cannot guarantee there will be no cyber-breaches. What we can do, and have done, is to take the best precautions reasonably possible so as to secure the data in those cases which are conducted using the DEF Platform. The Platform affords a high degree of data protection for neutrals and parties and parties' representatives' data in cases on the Platform.

Users have their part to play in preventing cyber-breaches. Users should:

a) Adopt and act in accordance with a password policy which involves the use of strong passwords and the Platform requires users to adopt strong passwords.
b) Change passwords regularly and not shared or left on notes on desks where the password may easily be seen; and,
c) Only communicate via the Platform concerning any documents uploaded onto the Platform and abide by the requirement in these User Terms at paragraph 6 to exchange all documents via the Platform.

13. Cessation of e-filing service

The Provider will not be liable to the User in damages or costs for any interruption in the Service:

(i) for any reason beyond its control; and,

(ii) the Provider's failure for any reason or for any period to provide the e-filing service shall not give rise to any liability on the part of the Provider.

14. Users acknowledge that the Provider may withdraw the e-filing service on 4 weeks' written notice at any time.

15. If the System's software or data storage service providers should at any time in future cease to provide the current e-filing service for any reason then registered Users agree that the Provider may at its absolute discretion:

(i) recreate the System by using a different or substitute software provider; or,

(ii) notify the User that e-filing is no longer available and the User will continue the case on paper. In this event the e-filed documents for each case will all be destroyed forthwith by the Provider; and,

(iii) because each User is required to keep back-up copies of all e-filed documents and communications on each individual file the Provider shall not be liable to return any copies of e-filed documents to any User.

16. Substitute software

In the event of withdrawal of the e-filing service DEF will notify Users by email to the email address registered on the Platform for each User that DEF is making efforts to arrange for the redesign and recreation of the System and to provide it to Users within 56 days of that notification being sent.

17. In these circumstances no guarantee is given by DEF that there will not be an interruption in the provision of the Service and no liability will follow if there is such an interruption.

18. If DEF is unable for any reason to re-create and to provide the e-filing service after the 56th day of any such period of service interruption then the Provider will notify Users forthwith by email and the efiling service will terminate without any liability between Users and the Provider.

19. Variation of User Terms

These User Terms will be varied from time to time save as restricted by the Standard Contractual Clauses in the Appendix hereto. DEF will notify all registered Users by email of such variation the time the changes are introduced. Users' continued activity on the Platform after such variation will be taken as acceptance of the varied terms of use.

Valid from 1 November 2019

END SAVE FOR THE APPENDIX

THE APPENDIX

The Standard Contractual Clauses for international transfers from Controller to Controller

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

Between:

The User or Users at the address and with the contract details provided during the Users' registration (the data exporter, being an individual or entity established within a Member State of the EU)

DEF and its registered address is as provided at the foot of the registration/login page on the Platform at https://oneplatform.disputesefiling.com/ (the data importer)

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "the data exporter" shall mean the controller who transfers the personal data;

(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.
(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data

importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the

data importer (the authority), which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data in accordance with the data processing principles set forth in Annex A.

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each

other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required. This prohibition extends only to the Standard Contractual Clauses in this Appendix and does not act to prohibit variation of the User Terms otherwise.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: the date on which the Users/parties accept these User Terms and thereby these Standard Contractual Clauses.

ANNEX A

DATA PROCESSING PRINCIPLES

1.

Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2.

Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3.

Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4.

Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5.

Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on

unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6.

Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7.

Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8.

Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

(a)

(i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

(ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or,

(b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

The System will store all of the users/parties' personal details such as names and addresses and their e-filed documents some containing specific, identifiable health data and data relating to children. The System will not use or process (other than storing) the information in these documents in any way beyond e-storage for the relevant services provided by the Platform.

COMMERCIAL CLAUSES WHICH FORM PART OF THE USER TERMS

Indemnification between the data exporter and data importer:

The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the "indemnified party(ies)") promptly notifying the other party(ies) (the "indemnifying party(ies)") of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.

Dispute resolution between the data exporter and data importer*:*

In the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be finally settled under the rules of arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be as agreed between the parties. The number of arbitrators shall be 3."

Allocation of costs:

Each party shall perform its obligations under these clauses at its own cost.

Further obligation upon termination:

In the event of termination of these clauses, the data importer must return all personal data and all copies of the personal data subject to these clauses to the data exporter forthwith or, at the data exporter's choice, will destroy all copies of the same and certify to the data exporter that it has done so, unless the data importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The data importer agrees that, if so requested by the data exporter, it will allow the data exporter, or an inspection agent selected by the data exporter and not reasonably objected to by the data importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours.

END OF APPENDIX