MyDPAM
SPECIFIC TERMS AND CONDITIONS
3 OCTOBER 2018

1. INTERPRETATION, STRUCTURE AND OBJECT

1.1. Interpretation

1.1.1. The use of MyDPAM is governed by (i) these Specific Terms and Conditions, (ii) the Subscription Agreement, and (iii) the General Terms and Conditions.

1.1.2. The words and expressions starting with a capital letter are defined in Article 2 below.

1.2. Structure

1.2.1. In the event of any conflict or inconsistency between the General Terms and Conditions and the Specific Terms and Conditions, the Specific Terms and Conditions shall prevail. The Specific Terms and Conditions are available in English, French and Dutch. The legal value of each version is the same regardless of the language used.

1.2.2. DPAM has made available on the website of MyDPAM the documentation referred to in this Specific Terms and Conditions for the consultation by the Client and the Authorised Users. The Client and/or the Authorised Users have the right to request these Specific Terms and Conditions in paper format or on any other durable medium during the term of the Subscription Agreement.

1.3. Object

1.3.1. These Specific Terms and Conditions set out the rights and obligations of the Client, the Authorised Users and/or DPAM in relation to the use of MyDPAM and the Services proposed there in.

1.3.2. The Client and the Authorised User acknowledge and accept that the use of MyDPAM is governed by these Specific Terms and Conditions, the Subscription Agreement, and the General Terms and Conditions.

2. DEFINITIONS

"Account"

Any account opened by a Client for the recording and safekeeping of financial instruments and liquidities in accordance with the applicable laws and regulations. For the avoidance of doubt, (i) the functionalities of MyDPAM are for consultation purposes only; (ii) MyDPAM does not propose functionalities allowing to make payments or transactions.

"Authorised User"

Any person duly authorised by the Client to use and access MyDPAM.

"Client"

Any client of DPAM to whom DPAM is providing investment services in accordance with the Belgian act of 2 August 2002 on the surveillance of the financial sector and financial services, as this may be amended from time to time.

"Device"

Any device (computer, tablet or mobile phone) used by the Authorised User to access via internet the Services.

"Digital Care"

The first line support made available by DPAM to the Clients or the Authorised Users for the use of MyDPAM. Further information on Digital Care is available in the User Guide.

"DPAM"

Degroof Petercam Asset Management, a public limited liability company with registered offices at 18 Rue Guimard, 1040 Brussels, Belgium and registered with the Brussels Register of Legal Persons (RPM) under number 886.223.276.

"GDPR"

The regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as this may be amended from time to time.

"General Terms and Conditions"

The general terms and conditions governing the business relation between DPAM and its Clients, as these may be amended from time to time.

"Mobile Application" or "Application"

The computer application required to access and use MyDPAM via a Device belonging to the Authorised User.

"MyDPAM"

The internet platform made available by DPAM to its Clients and/or the Authorised Users for the provision of the Services as further described below.

"Privacy Policy"

The privacy policy issued by DPAM whereby DPAM provides additional information on the way DPAM treats the personal data of individuals, the rights of individuals for protecting their data and the way such rights may be exercised, as this may be amended from time to time.

"Secured access"

The different types of secured access used by the Authorised Users to securely log in their personal space of MyDPAM. The access to MyDPAM may be made with (i) a Smartcard, or (ii) QR code, or (iii) any other means of secured access provided by MyDPAM to the Authorised Users from time to time.

"Services"

The services available on MyDPAM from time to time. For the avoidance of doubt, DPAM may change at any time the Services proposed based on its own assessment of the Client’s needs. The Services include, but are not limited to:

- **Portfolio consultation**

(i) Explorer: it allows the Authorised User to, amongst other, (i) consult the list of portfolios relating to the Account and (ii) create groups of portfolios relating to the Account.

(ii) Dashboard: it allows the Authorised User to, amongst other, consult a dashboard presenting the data relating to the portfolio Account according to different angles: portfolio valuation evolution, portfolio income, portfolio performance (monthly performance year to date and performance by calendar year since inception), portfolio breakdown by asset category, portfolio breakdown by currency.

(iii) Positions

- Analysis grid: it allows the Authorised User to, amongst other, consult the data relating to the portfolio Accounts based on an analysis grid.
- DPAM funds: it allows the Authorised User to, amongst other, access the various legal and marketing documents as well as the main portfolio statistics linked to the Account.

(iv) Transactions: it allows the Authorised user to, amongst other, consult the history of transactions related to a specific instrument included in the portfolio Account (with a maximum of 10 years of history starting at the date of portfolio performance migration).

(v) History: it allows the Authorised User to, amongst other, consult the history of the portfolio Account presenting the evolution over time in terms of currency and asset classes (with a maximum of 10 years of history starting at the date of portfolio performance migration).

(vi) Information: it allows the Authorised User to, amongst other, consult information to specific references in the portfolio Account as well as some additional market data such as the spot exchange rates of the main currencies versus the reference currency.

"Smartcard"

An electronic device that issues a single time use code. DPAM will provide each Authorised User with a Smartcard.

"Specific Terms and Conditions"

These Specific Terms and Conditions whereby DPAM sets out the terms for the use by the Authorised Users of MyDPAM.

"Subscription Agreement"

The subscription agreement executed between DPAM and the Client whereby (i) DPAM and the Client set out, and agree to be bound by, the terms of service governing MyDPAM, and (ii) the Client designates the Authorised Users.

"User Guide"

Any manual that may be accessed by the Authorised User (either online or on paper) and containing some conditions and technical guidelines for accessing and using the Services.

3. CONDITIONS OF ACCESS TO THE SERVICES

3.1. General

3.1.1. MyDPAM may be accessed by the Client and/or Authorised User via the internet at (https://www.mydpam.com) or via the Mobile Application. The procedure to access MyDPAM is further explained in the User Guide.

3.1.2. The Client and/or the Authorised User shall use the Services in compliance with the rules set out in these Specific Terms and Conditions, the General Terms and Conditions, the User Guide and any other information or instruction provided by DPAM by post, e-mail or any other means.

3.2. Security measures

3.2.1. DPAM reserves the right to refuse access to the Services or to terminate or suspend access to the Services under the conditions set out in these Specific Terms and Conditions. In particular, and without prejudice to any other provisions of these Specific Terms and Conditions, DPAM may decide to block access to MyDPAM, with immediate effect and without prior notice, in the following case(s):

- The Authorised User has not installed the latest update of his/her internet browser or Mobile Application;
- The Authorised User's Device does not comply with the safety instructions set out in the User Guide, these Specific Terms and Conditions and/or the General Terms and Conditions;
- The protection features of the Authorised User's Device, which would enable the Services to be used safely, have been deactivated;
- The Authorised User has not followed the safety instructions given by DPAM directly or set out in the User Guide, these Specific Terms and Conditions or the General Terms and Conditions;
- The Authorised User repeatedly enters into the Application several times the wrong Secured Access codes, or adopts any other unusual or erratic behaviour that creates a reasonable suspicion of attempted fraud;
- DPAM has detected or been informed of potential fraud or misuse of the Services.

3.2.2. If the access to MyDPAM of an Authorised User is blocked, the Authorised User DPAM shall immediately contact the Digital Care to enquire about the reasons that resulted in his/her access to MyDPAM being blocked, and if applicable, the procedure to follow to re-establish his/her access.

3.2.3. DPAM is at all times authorised to implement new Secured Access means and to amend the means and procedures for accessing MyDPAM in order to optimise the security of its systems, its Mobile Application and its website. DPAM will duly inform the Authorised Users of any new Secured Access.

4. USE OF SERVICES

4.1. Operating hours

4.1.1. The Authorised User has access 24 hours per day, seven days a week, without prejudice to the provisions provided in these Specific Terms and Conditions.

4.1.2. DPAM may suspend access to these Services at any time for the purposes of:

- carrying out maintenance or improving the Services; or
- making improvements to its computer system; or
- fixing or preventing any machine, software or communication equipment breakdowns or failures (including in the event of attempted hacking or embezzlement).

4.1.3. Access to the Services may also be suspended in the event of a technical problem or network overload, the cutting of telephone lines, errors, negligence or faults on the part of a third party or the Authorised User, in particular, when installing and using the Services, as well as any other circumstances that are beyond DPAM's control or in the case of force majeure.

4.1.4. DPAM cannot guarantee access to the Services if there is a considerable or unexpected increase in the volume of use of MyDPAM.

4.1.5. If the Services are intentionally blocked by DPAM, DPAM may authorise the access and use of MyDPAM again at its own discretion.

4.1.6. DPAM will make every effort to limit the maximum period of interruptions of access to the Services and to inform the Authorised User of the day and time, as well as of the period, of disruption.

5. Identification

5.1. The procedure to access MyDPAM is explained in detail in the User Guide. The Authorised User is required to identify himself/herself with the assistance of the Secured Access means provided by DPAM.

5.2. The Authorised User acknowledges that the Secured Access, including any technical means of identification and signature made available or authorised by DPAM for the Authorised User to access and use the Services, are considered an electronic signature within the meaning of the law and are valid proof of the Authorised User's identity.

5.3. DPAM is entitled to consider any person who accesses MyDPAM by means of the Secured Access to be an Authorised User. The Client acknowledges that any request made on MyDPAM using Secured Access is assumed to originate from an Authorised User.

5.4. If DPAM informs the Client and/or the Authorised Users of a problem relating to the Secured Access, the Client and the Authorised User are solely responsible for any further use of MyDPAM if the Secured Access have not been modified or adapted by the Authorised User in accordance with DPAM’s injunctions.

6. CLIENT AND AUTHORISED USERS’ OBLIGATIONS

6.1. The Client shall ensure that the Services are used by the Authorised User with due diligence, and shall ensure that the Authorised User fully complies with the instructions and obligations set out in the User Guide, any updates to the User Guide and any information and instructions provided by DPAM on its website, via the Mobile Application or by any other means, such as a letter, e-mail or Account statement.

6.2. The Client shall ensure that the Authorised User keeps the Secured Access codes secret and confidential. The Client shall take appropriate steps to ensure that the Secured Access codes are not disclosed to any unauthorised person.

6.3. The Client shall, at its sole responsibility, ensure that the organisation, surveillance and control mechanisms are in place to ensure the safety and confidentiality of the Secured Access codes of his/her/its Devices and of the Mobile Application. To that end, the Client shall ensure that:

- any standard and recommended protection systems for his/her/its computer or internet system are in place (firewall, antispyware, anti-virus, etc.);
- any available updates for the operating system of his/her Device and any available updates for the operating system for the Mobile Application are installed;
- jailbroken or rooted Devices are not used;
- passwords used to access Devices are not a combination that is too simple, for example, 111111, 12345, or a very common word (such as "password") or relate to personal information (date of birth, etc.);
- he does not allow third parties (including family members or friends) to access MyDPAM.

6.4. The Client and the Authorised Users undertake to take all measures to protect the confidentiality of the Secured Access notably:

- any means used to access the Services are in a safe place and not available to a third party, including family members and friends;
- any appropriate measures are taken, when the Authorised User has requested access to MyDPAM, to ensure that he/she will receive the confidential Secured Access codes personally;
- memorise the Secured Access codes and/or keep them confidential;
- any Secured Access codes are not a combination that is too simple, for example, 111111, 12345, or a very common word (such as "password") or relate to personal information (date of birth, etc.);
- not to communicate the Secured Access codes under any circumstances to third parties (including family members or friends) and never to allow third parties to use them; no-one, including a bank, has the legal right to ask the Authorised User to disclose his/her Secured Access;
- not to write down the Secured Access codes in a way that is easily recognised or even in coded format, on or near the Device used for online consultation;
- to only use the Secured Access codes in a safe place where there is no one else looking and there are no distractions.

6.5. The Authorised User is exclusively responsible for ensuring that the computing equipment and software of his/her device, and the telecommunication system, comply with the specifications provided in the User Guide.

6.6. The Authorised User must inform DPAM if he/she becomes aware that:

- the Secured Access have been lost or stolen, or if they are not received within a reasonable time if sent by post; or
- his/her Devices have been lost or stolen or used without authorisation; or
- a transaction has been carried out without his/her consent; or

- an error or irregularity appears in MyDPAM.

6.7. Notification in the cases mentioned above must be given via Digital Care. If the Authorised User does not take these precautions, he/she is responsible for the fraudulent use of his/her Secured Access.

6.8. In the event that the Digital Care service is not available, the Authorised User shall make this notification as soon as this service is available again or shall contact DPAM using any other means.

6.9. The Authorised User acknowledges having been informed by DPAM of the technical measures and minimum configurations required to ensure secure access to the Services.

7. OBLIGATIONS OF DPAM

7.1. DPAM will make all reasonable efforts to ensure the Authorised User can access and use MyDPAM, without prejudice to any other article of these Specific Terms and Conditions.

7.2. DPAM’s commitments towards the Authorised User within the context of MyDPAM constitute best efforts obligations. DPAM shall take all reasonable measures to ensure that Authorised Users are provided with a regular service and appropriate identification and authentication methods.

7.3. DPAM shall ensure that security systems in compliance with recent technical developments are put in place and are maintained in order to:

- protect MyDPAM and the Mobile Application against any known viruses and digital fraud;
- prevent the interruption, termination or malfunction of MyDPAM;
- prevent any theft, loss, destruction or modification of the data and logistics or digital equipment following the illegal access of DPAM's or Authorised User's computing system by a third party, and following a virus from DPAM's or Authorised User's website, internet, or computing system.

7.4. DPAM shall ensure that the Authorised User is able to make the notification stated in Article 6.6 of these Specific Terms and Conditions.

7.5. DPAM reserves the right to employ sub-contractors to provide the Services of MyDPAM.

8. LIABILITIES OF DPAM

8.1. The liability of DPAM regarding the Services is governed by the provisions on this subject in the General Terms and Conditions and by the provisions below.

8.2. Information and statements made available on MyDPAM may differ from the actual situation of the Account. Such situation may arrive when there is a time lag between the execution of a transaction, the recording of a transaction and their respective display on MyDPAM. DPAM cannot provide any guarantee as to the immediate display on MyDPAM of information following the execution and/or the recording of a transaction. A delay in the display of information relating to a transaction may result in a temporary inaccurate view of the Account. DPAM shall not be held liable for delays in the display of transactions on MyDPAM.

DPAM will do its outmost to ensure that transactions appear on MyDPAM as quickly as possible.

8.3. DPAM uses information collected from different external sources to provide Services on MyDPAM. In relation to the information collected from external sources, DPAM considers that the information is reliable and does not give any guarantee whatsoever as to its correctness, consistency, completeness, reliability, availability, marketability or suitability.

8.4. Except in the case of wilful misrepresentation or gross negligence of DPAM, DPAM is not liable and will not be required to indemnify the Client nor any Authorised User for any direct or indirect damage that he/she/it may have incurred as a result of, but not limited to:

- the interruption, termination or malfunction of MyDPAM;
- the disclosure of the Secured Access to non-authorised users or to a third party or from the misuse of the Secured Access by the Authorised User or a third party;
- any theft, loss, destruction or modification of the data, software or computer hardware of the Authorised User as a result of the unlawful access by a third party to the computer system of DPAM, of the Authorised User, as well as resulting from a virus originating from the website, the internet, the computer system of DPAM or of the Authorised User;
- abusive use of MyDPAM by the Authorised User or third parties;
- malfunction of a Device or of the telecommunications services supplied by a third party;
- the lack of foresight or non-compliance with instructions from, or security precautions communicated by, DPAM with respect to the use of MyDPAM, Secured Access, any Devices, internet browser, firewall, anti-virus or operating system;
- any reason beyond the control of DPAM, including any event of force majeure, that is any unexpected event beyond the control of DPAM and which could not have been reasonably avoided and which prevents or delays the implementation by DPAM or any other person acting on its behalf, of certain obligations stated in these Specific Terms and Conditions, including natural disasters, the outbreak or escalation of hostilities (regardless of whether or not war has been declared), hacking or cyber-attack which could not reasonably have been prevented by reasonable security measures, any illegal act against public order or authority, all unforeseeable acts by the authorities, strikes or other employment conflicts, government restrictions, cuts in power or communications, suspension of payments, insolvency, sequestration or administration orders, bankruptcy or liquidation of any third party.

8.5. DPAM will assume the risks of sending the Secured Access to the Authorised User. After receipt the Client and/or the Authorised User shall be liable for any consequences of the usage thereof subject to the limits and conditions described in Article 9.

9. LIABILITIES OF THE CLIENT AND/OR THE AUTHORISED USER

9.1. The Client and/or the Authorised User is fully and personally liable for the proper functioning of his/her Devices and additional equipment required (modem, internet access, etc.) and for the connection of the Devices to the internet.

9.2. The Client and/or the Authorised User shall bear all consequences of unauthorised access to Services if this is due to fraudulent or intentional actions or gross negligence on his/her part. Gross negligence includes, in particular, cases where the Authorised User does not comply with the obligations described in Article 6, such as writing down the Secured Access codes in an easily recognisable format, in particular on an object or a document being kept or taken along by the Authorised User, or not reporting the loss or theft as soon as the Authorised User and/or the Account holder became or should have become aware of it.

9.3. The Client and/or the Authorised User shall follow all the obligations allocated to them by these Specific Terms and Conditions, any other contractual document to which the Client and/or the Authorised User are bound or any document that is communicated by DPAM to the Client and/or Authorised User.

9.4. The Client and the Authorised User shall hold DPAM harmless for any damage resulting from the failure by the Client and/or the Authorised User to comply with his/her obligations to DPAM when using MyDPAM, without prejudice to the respective right of recourse of DPAM or the Client against the Authorised User. The Client shall indemnify DPAM for the actions of his/her Authorised Users.

9.5. When the Authorised User uses his/her Secured Access for purposes of identification, he/she does so under his/her sole responsibility. The Authorised User therefore assumes sole responsibility for access to MyDPAM after identifying himself/herself using the Secured Access, including by any third person accessing with our without authorisation the Authorised User's Device.

10. FEES AND EXPENSES

10.1. DPAM shall not bill the Client for the usage of MyDPAM.

10.2. The Client or the Authorised User shall bear any costs relating to his/her Devices or equipment required to use the Services, as well as any installation, reparation or replacement costs associated with the use of MyDPAM.

10.3. Any costs associated with an internet subscription and mobile connection in Belgium or abroad is considered as incurred by the Authorised User and shall be paid by the Client or the Authorised User.

11. PRIVACY AND DATA PROTECTION

11.1. The Client confirms that it is allowed and, consequently, that it has a valid legal basis, as required by GDPR, to share the personal data of Authorised Users with DPAM so that DPAM (or any third party appointed for such purpose) can record and process such personal data in the framework of the services to be provided by DPAM via MyDPAM for the purposes of managing the contractual relationship and the portfolio, ensuring compliance with regulatory requirements such as investor protection, prevention of money laundering and funding of terrorism, abuse or fraud, commercial prospecting (including direct marketing), and ensuring the proper functioning of the services proposed and any enhancement thereof.

11.2. Given that DPAM does not have direct contractual relationship with the Authorised Users, DPAM hereby delegates, and the Client hereby agrees, to carry out DPAM's obligation of information under GDPR towards any Authorised Users. In this respect, the Client shall:

- ensure that Authorised Users are properly informed in accordance with GDPR that personal data relating to them will be used, disclosed or otherwise processed by DPAM and/or any third party appointed by DPAM to develop MyDPAM and that Authorised

Users are informed that the treatment of their personal data is made in accordance with the Privacy Policy;

- develop and implement appropriate procedures for timely handling complaints or requests by Authorised Users to exercise their subject access or other rights under GDPR and for cooperating with DPAM in the event the DPAM receives such requests directly from any Authorised User.

11.3. Authorised Users may refer to the Privacy Policy for additional information on the rights they have relating to the processing of their personal data and the way such rights can be exercised. The Privacy Policy is available on the website of MyDPAM.

12. COOKIES

12.1. MyDPAM makes use of cookies. A cookie is a small data set sent by a website (ex MyDPAM) to a web browser and is stored locally on the visitor's computer or electronic device where this web browser software is running (ex on the Authorised User's Device). For additional information on cookies and their functioning please refer to other internet sources, such as Wikipedia or http://www.allaboutcookies.org/.

12.2. MyDPAM uses the following type of cookies: (i) functionality: to save information such as the Authorised User's language preference, so that he/she is automatically directed to the information required in the language chosen during the first visit. These cookies are never used for any other purpose, (ii) authentication: to know whether the Authorised User is logged in or not and determine from which Account they are logging-in; (iii) technical: to manage the structure required by MyDPAM and be able to provide the services requested by the Authorised User.

12.3. The cookies can be deactivated by the Authorised User by changing the browser's settings. Information on how to change the cookies settings in the browser is available in the browser's help section. All cookies may be deactivated by the Authorised User. However, the consequence of deactivating cookies varies depending of the type of cookie deactivated. Deactivating functionalities cookies will have a lower impact on the Authorised User's navigation. For example, the browsing experience on MyDPAM will result in a less personalised experience and the Authorised User will be required to select the country and language preference each time he will long in on MyDPAM. Deactivating authentication and technical cookies have a major impact on the functioning of MyDPAM and their absence will result in MyDPAM not working. These types of cookies are considered as strictly necessary and must remain authorised to be able to make use of the Services.

12.4. By accepting these Specific Terms and Conditions, the Authorised User acknowledges and accepts to the use of the cookies described above and commits to authorised them.

13. INTELLECTUAL PROPERTY

13.1. The use by the Client or the Authorised Users of the Services on MyDPAM may not and shall not result in any way in the Client or the Authorised Users becoming owner of the intellectual property rights, including copyright, database rights, software rights and any know-how relating to the software, programs, Application, User Guide and any other documents made available or merely accessible in connection with MyDPAM.

13.2. The Client and/or Authorised User obtains only a right of non-exclusive and non-transferable usage of the Services for his/her/its own personal needs.

13.3. The Authorised User undertakes to use the Services in accordance with the instructions and directions of DPAM and may not, in any form or fashion whatsoever, whether free of charge or against payment:

- make them directly or indirectly available to third parties;
- reproduce them, copy them in whole or in part;
- process, translate, adapt or alter them;
- transfer, assign, license, rent, loan or distribute any component of the Mobile Application, including the software which is linked to them and their documentation;
- use them in order to create software or any other application which is functionally equivalent to all or part of them;
- use them in a manner which could lead to the encouragement, obtaining or performing of any illegal or criminal activity or which could cause damage or injury to any other person; and/or
- withdraw, obscure or alter the display of the property rights shown on the documents.

13.4. More generally, the Authorised User undertakes to comply with all property rights, particularly intellectual property rights, of DPAM, its sub-contractors or any other relevant persons.

13.5. The Authorised User may not transfer the rights and obligations resulting from this agreement to any third parties.

14. AMENDMENTS

14.1. DPAM reserves the right to unilaterally modify these Specific Terms and Conditions at any time. Any amendments made by DPAM to these Specific Terms and Conditions will be communicated to the Client and to the Authorised User by letter, e-mail, communication via the website or Mobile Application, or any other suitable means.

14.2. The Authorised Users are required to consent to the Specific Terms and Conditions of MyDPAM upon their first connection and each time these are updated. DPAM is authorised to consider that the use by the Authorised Users of MyDPAM entails acknowledgment and acceptance by the Authorised User of the Specific Terms and Conditions of MyDPAM. If the Client or the Authorised User do not consent to the changes made to the Specific Terms and Conditions, they shall have the right to terminate the agreement for the Services of MyDPAM by following the procedure described in Article 15.

14.3. Notwithstanding the above, it is understood that any amendments relating to the Secured Access and/or the security measures taken by DPAM to secure MyDPAM will take effect as soon as they are communicated to the Client and/or Authorised User by letter, e-mail, communication via the website or Mobile Application, or any other suitable means. If the Authorised User accesses the Services for the first time after receiving notification of the above-mentioned amendments, DPAM may conclude that the Authorised User has fully approved them.

15. TERM AND TERMINATION

15.1. The Client and/or the Authorised User subscribe to the Services of MyDPAM for an indefinite period.

15.2. The Client may terminate this agreement at any time by informing DPAM of his desire to terminate the agreement relating to MyDPAM.

15.3. DPAM may terminate this Agreement by written notice of 1 month, without prejudice to Article 15.4 below.

15.4. In case of wilful misrepresentation or gross negligence by the Authorised User, when the Authorised User does not comply with the security measures and the terms of these Specific Terms and Conditions, or when the Authorised User is responsible for acts that could jeopardize the relationship of trust with DPAM, DPAM is entitled to terminate the Services with immediate effect, without prejudice to any compensation that may be owed to DPAM by the Authorised User.

16. COMPLAINTS PROCEDURE

16.1. Users wishing to make a complaint about MyDPAM shall comply with the procedure described in the General Terms and Conditions. The General Terms and Conditions are available on MyDPAM.

17. APPLICABLE LAW AND JURISDICTION

17.1. These Specific Terms and Conditions are governed by Belgian law. Subject to the mandatory provisions applicable to consumers, in the event of a dispute, the competent courts will be the courts of Brussels.