PROTOCOL

FAD
Fraude Aanpak Detailhandel

The Dutch Data Protection Board of that time issued a statement of lawfulness, as required under Article 22, opening lines and subsection 4(c), in conjunction with Article 31, opening lines and subsection 1(c), of the Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens, Wbp).

- **Initial statement of lawfulness granted on:** **24 June 2004**
- **Second statement of lawfulness granted on:** **10 July 2008**
- **Third statement of lawfulness granted on:** **25 November 2014**

PROTOCOL

Version 4.0

Foundation for Fraud Prevention in the Retail Trade (*Stichting Fraude Aanpak Detailhandel*)

1. Introduction

1.1 A brief history

Every year, the retail trade is confronted with a considerable amount of losses. This is estimated to involve an amount of over €250 million annually. This involves losses due to shoplifting and fraud committed by retail businesses' own or hired staff. Therefore, retail businesses are also being damaged, unfortunately, by forms of internal fraud from within their own ranks. In order to actively combat this type of damage, the Foundation for Fraud Prevention in the Retail Trade (*Stichting Fraude Aanpak Detailhandel, Stichting FAD*) was set up in 2004 on the initiative of the Dutch retail association formerly known as *Raad Nederlandse Detailhandel* (currently: *Detailhandel Nederland*). The purpose of the Foundation is to actively tackle internal fraud by maintaining a national warning register recording a few personal details of persons who were employed by, or worked at, affiliated participants and were dismissed due to internal fraud or with whom the employment relationship has been terminated and who have been reported to the police for a criminal offence. When filling existing vacancies, businesses participating in the national warning register can check to find out whether a job applicant was ever dismissed by another participant due to internal fraud. Thus by using the register, these employees who have been dismissed are prevented as much as possible from easily finding a job at another retail operation.

The conditions governing the way this warning register functions, as well as how affiliated retail businesses and shop owners report information and use the register, have been laid down in a Protocol with accompanying Notes. When the register was set up, the provisions of the Protocol were formulated in accordance with the requirements of the Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*, Wbp), the applicable statutory regulations at the time. When registering, the authorised director of each retail business or shop owner must declare that they will strictly follow the rules of this Protocol and the Notes. An Audit Committee monitors the correct use of the register in accordance with the provisions of the Protocol. Pursuant to the legally enshrined requirements, the final step in protecting the legal position of the persons involved is a Complaints Committee set up to handle complaints of persons who have been recorded in the warning register, if these persons have not been able to come to a mutually suitable solution in consultation with their former employer or work placement provider/hirer. The warning register became operational in June 2005. Five affiliated retail chains were the first to sign up, which has now expanded to 64 retail chains, with the addition of 953 SME retailers affiliated via their sector service association. Besides the nationally operative retail chains, at present smaller SME businesses with one or several shops can also register through several sector service associations. At present, the warning register covers 245,000 employees who work in the Dutch retail trade.

Initially, only a company's own personnel who were dismissed on account of fraud and a reported offence could be recorded in the register. Subsequently, work placement students and temp agency workers were first incorporated into the functioning of the Warning Register, while later other categories of persons actually active at the workplace of participating businesses followed. This concerns self-employed worker without employees, payrollers, concessionary staff and other persons working on a temporary basis in retail who are not in the permanent employment of the participant. The retail trade has increasingly transitioned to working with a temporary external workforce. The Warning Register has adjusted in step with this development so that it remains a relevant instrument for combating fraud 'from within' even in these changed circumstances. The Protocol has been continually amended in response to this broadening of the scope of the Warning Register. This development was effected with the consent of the then Dutch Data Protection

Authority, who conducted a preliminary investigation before the Register became operational. A statement of justification has always been issued for the changes to the Protocol described here, the last one being issued in 2016. On the grounds of the transitional regulation of Article 48, paragraph 11, of the General Data Protection Act (GDPR) Implementation Act, such a statement applies automatically as a licence within the meaning of Article 33, paragraph 4(c), of said Act. Since the Dutch Data Protection Authority issued this statement in 2016 for an indefinite period, the required licence is also in force for an indefinite period under the current GDPR regime.

It may be said without exaggeration that the Warning Register has acquired an important place in tackling the problem of losses in the affiliated retail businesses due to internal fraud committed by their own and hired personnel.

1.2 Reasons for revision

There are currently reasons for revising the Protocol and its accompanying Notes once again. Various developments have played a role in this. Firstly, there have been changes to the applicable legal framework. The Personal Data Protection Act has been replaced by the General Data Protection Regulation (GDPR). This EU regulation has direct effect in all EU Member States and therefore also forms the legal framework for the protection of personal data in the Netherlands in processing such as the Warning Register. The GDPR entered into effect on 25 May 2018. The national GDPR Implementation Act entered into effect in response to this, which regulates, among other things, the transitory provisions, the repeal of the Personal Data Protection Act, and the creation of a Data Protection Authority as regulator. Further, a legal regulation has been created which is usually referred to as the Data Breaches (Reporting Obligation) Act. Following the entering into effect of this new legal framework, the necessary measures were rolled out to ensure that the Warning Register became ‘GDPR-proof'. Thus, the Audit Committee drew up an assessment document which indicates how the conditions and obligations of the GDPR are fleshed out in the Warning Register. Moreover, a new processing agreement has been concluded with the processor of the system, and a procedure has been set up for reporting data breaches. These actions have now been completed. bringing the Register in line with the new legal framework. But the Protocol still had to be amended. The current 2020 version provides the necessary amendments.

In addition, the experience of the Audit Committee and Complaints Committee have revealed certain aspects that require further regulating. The changes pertain to expanding the duties of the Audit Committee in line with the regulations of the Data Breaches (Reporting Obligation) Act and sanctions governing cases involving shortcomings and serious defaults by participants in complying with the Protocol. The Complaints Committee ran into the problem that there were as yet no provisions for proper regulation of the record-keeping requirement relating to persons who had been entered in the Warning Register by participating companies which had undergone reorganisation or liquidation, or which had withdrawn. These items also demand that specific regulations be incorporated into the Protocol.

It goes without saying that the Notes to the Protocol also had to be brought up to date with the revisions. The texts of both the Protocol and the Notes have been completely rewritten, even though a great deal of the existing text was taken over in the revision. In fact, the functioning of the Warning Register has not in essence been changed by the new legal framework of the GDPR.

1.3 The General Data Protection Regulation (GDPR)

Under the scope of the General Data Protection Regulation, a legal system exists in which a certain basis is required as pre-condition for processing personal data. The Warning Register is necessary for representing the **legitimate interests** of the controller, as referred to in Article 6, paragraph 1(f), of the GDPR. This basis can be further explained as follows.

In order to meet its **statutory objectives**, the Foundation for Fraud Prevention in the Retail Trade (*Stichting FAD*) has a justified interest in maintaining its processing of personal data in the Warning Register. The *Stichting FAD* has set itself the objective of reducing the phenomenon of internal fraud by a company's own or hired personnel working at affiliated retail businesses. The losses due to various forms of theft, including internal fraud and other criminal damage, is estimated at over €250 million annually. In view of **these substantial losses**, businesses in the retail trade, both retails chains and small businesses, have a considerable interest in combating fraud committed by their own or hired staff. The *Stichting FAD* has been offering an **effective instrument** for tackling such fraud since 2005 – the Warning Register, which can be used for registering staff dismissed due to internal fraud and temporary hires whose employment has been terminated and who have been reported to the police for committing an offence. By consulting the Register, the affiliated participant can check whether there are any objections to an applicant when recruiting or hiring new personnel (pre-employment integrity screening). Internal fraud has an extremely **detrimental effect** on the internal culture of businesses: it damages a good work atmosphere, leads to distrust among colleagues, sets the wrong example, and puts personal gain above loyalty to the company and respect for other people's property. It is also **breaches the trust** that every employer must invest in his/her staff. Because the *Stichting FAD* processes criminal records in the Warning Register on behalf of third parties (the participants), particularly in official reports to the police, a **licence** is required from the Personal Data Authority. In the foregoing, we already indicated that the *Stichting FAD* possesses such a licence on the grounds of a provision of the transitional regulation in the GDPR Implementation Act. The Warning Register meets the requirements of **proportionality** and **subsidiarity** in every other respect. No more personal data is processed than is strictly necessary (proportionality) and there is no other, less intrusive means available for achieving the intended aim (subsidiarity). The **'black list' phenomenon** that also applies to the Warning Register, if one wants, has now become **socially accepted** as a justified form of protection against property offences or other unacceptable behaviour in various different areas of society (insurance, transport, football, hospitality). Finally, it must be said that registration in the Warning Register does **not** lead to **disqualification from a profession**. The data subject in the Register retains many options for finding a different job in the job market, which, after all, offers more employment opportunities than only working at affiliated retail businesses.

Based on these considerations, and also in light of the success of the functioning of the Warning Register since 2005, the board of the Stichting FAD believes that this represents a justified interest within the meaning of the GDPR for the continued existence of the Warning Register.

2. Definitions

In the Protocol and accompanying Notes, the following terms have the following meanings:
Audit: a visit by one or more members of the Audit Committee to a participant in order to monitor the correct use of the Warning Register within the participant's organisation, in accordance with the provisions of the Protocol;

GDPR: The General Data Protection Regulation (Regulation (EU) 2016/679 of 27 April 2016, which entered into effect on 25 May 2018);
Board: the board of the Foundation for Fraud Prevention in the Retail Trade (*Stichting Fraude Aanpak Detailhandel*), which acts as the controller, in the terms of the GDPR, for the Warning Register;

Data subject: an individual natural person whose basic personal data has been entered in the Warning Register and who belonged to one of the following categories: staff in a participant's permanent or temporary employment; staff that was actually working at a participant's workplace on a temporary hiring basis, i.e. temporary agency staff, work placement students, self-employed workers without employees, personnel employed by a concessionaire or a payroll organisation;

Authorised persons: persons designated by the participant who are empowered to take decisions on behalf of the participant regarding inclusion of a person in the Warning Register, to conduct the associated proportionality test, to have access to the Warning Register, to work with the Register having received the necessary instructions from the participant;

Sector service association: intermediary who acts for an affiliated smaller business it represents and on their behalf enters this data or checks data in the Warning Register;

Corporate group relation: a participating organisation where the incident registers of subsidiaries of the participant or group companies are linked such that the incident register is accessible to each of these companies;

Concessionaire: a provider of products or services made available within a participant's retail space for sale of its products or services, or occupies space on a temporary basis for promoting and/or demonstrating its products or services;

Participant: the legal person or entrepreneur who has been accepted to participate in the Warning Register by the board and in that capacity gains access to the Warning Register, either directly or via a sector service association.

Record-keeping requirement: the obligation of every participant to maintain a complete record, on paper or electronically, of every registered person reported and entered for the purposes of retrieval procedure, audit and/or complaint procedure; 5

Incident register: a participant's data collection set up for its own use which contains all the cases of internal fraud or other objectionable actions committed within the company and which only functions in the event of a transfer as a source for the Warning Register;

Hired staff: staff who actually work under the authority of the participant in his or her company without having an employment contract with the participant;

Integrity test: when a participant consults the Warning Register in the framework of the recruitment process for new personnel (pre-employment screening);

Internal fraud: any illegal act committed against the participant, a staff member or a third party, whether or not in collusion with others, aimed at obtaining a financial benefit for oneself or for others by removing and appropriating money and/or goods (including commercial information) which are the property of the participant, staff member or third party. Theft, (employee) embezzlement, forgery of documents and swindling are the most common forms of fraud committed by employees in the retail trade;

Participant's organisation: the participant's company, the participant's subsidiaries (as referred to in Section 24(a) of Book 2 of the Dutch Civil Code, or the group companies with which the participant is associated as one economic unit (Section 24(b) of Book 2 of the Dutch Civil Code);

(Primary) source: the participant who (first) entered the data regarding an individual natural person in the Warning Register and who is approached by another participant for the purposes of screening after a positive result within the context of a retrieval procedure;

Proportionality test: a well-founded decision about whether a person's data should be entered in the Warning Register following internal fraud, and, if the data is entered, about a suitable retention period for the information based on a careful consideration of all the relevant facts and circumstances of the case;

GDPR Implementation Act: the General Data Protection Regulation Implementation Act (Bulletin of Acts and Decrees 2018, 144);

Processor: someone who processes personal data on behalf of the board or a participant without being subject to the immediate authority of the board or a participant.

3. Accession of new participants

3.1 The board shall set the requirements, procedure and forms for the accession of new participants. Applicants who wish to become participants shall receive information about the functioning of the Warning Register, the rights and obligations of participants, and the costs in advance.

3.2 The board shall only accept businesses and entrepreneurs active in the **retail trade** as participants. This requires that the applicant is actually actively involved in supplying products and/or services to individual customers from a sales area, website, warehouse or office. In addition, the board may grant a **licence** to organisations outside the retail trade to make use of the format for the layout and organisation of the Warning Register, if need be in an amended form. 6

3.3 If the board decides that the applicant meets all the requirements, it shall accept the applicant as a participant.

3.4 Once accepted, participants undertake that they will comply with, and that they will ensure their employees comply with, the Protocol and accompanying Notes when working with the Warning Register by signing a accession declaration.

4. Rights and obligations of participants

4.1 Following acceptance, participants have the right **to enter** data from their own incident register into the Warning Register, **to consult** the Warning Register within the context of a recruitment procedure, and **to use** the personal data found during screening as the basis of decisions regarding filling job vacancies in their own businesses. All other use of the Warning Register and/or data derived therefrom is prohibited.

4.2 Participants undertake that they will pay the **financial remuneration** set by the board for participation and use of the Warning Register, and for audits conducted in their businesses. Other financial obligations shall be set by the board for sector service associations.
4.3 Participants are further obliged **to provide** the board, the Audit Committee and the Complaints Committee with all requested **documentation and information** which these organs deem reasonably necessary for carrying out their duties (obligation to provide information).

4.4 Participants undertake in respect of other participants **to report** internal fraud **as much as possible** and **to supplement the Warning Register**, unless a weighing of interests comes down on the side of the data subject, or urgent reasons based on a carefully constructed staff policy are considered to be present that would preclude reporting and registration of the relevant information.

4.5 Participants shall be obliged in the framework of the retrieval procedure **to provide information** about persons registered by them (identity and background information) to other participants.

4.6 Participants shall be obliged to comply with the **record-keeping requirement** for one year after the registration of the data subject has been removed from the Warning Register (retention period).

4.7 In the case of **liquidation**, **cessation of business activities**, **reorganisation** or **termination of the participation** in the Warning Register, the participant will take the necessary measures in a timely manner to ensure that it will also be able to comply with the **record-keeping requirement** afterwards by transferring the records elsewhere for inspection.

5. Further conditions and obligations

5.1 **Costs**. Participants shall be charged according to a methodology to be determined by the board. Additionally, the board may charge for conducting audits.

5.2 **Reciprocity.** Participants undertake vis-à-vis the board and other participants to enter personal data as much as possible in the Warning Register, in accordance with the requirements of Article 7.3 and in compliance with the Protocol.

5.3 **Legal assistance**. Participants shall, if requested, provide legal assistance in the case of claims related to providing and using personal data in accordance with the Protocol. 7

5.4 Liability. The participant who causes damages by acting in conflict with the Protocol is liable for these damages, unless the actions cannot be imputed to the participant.

5.5 Indemnity clause. Participants indemnify the board for all claims and liabilities ensuing from actions in conflict with the Protocol.

6. Imposing sanctions

6.1 The board is authorised to impose sanctions on participants if a participant remains negligent in following the instructions of the Audit Committee, acts in conflict with the Protocol, severely damages the interests of the *Stichting FAD* and/or other participants through actions or negligence, or brings the integrity of the Warning Register into serious disrepute. Actions or negligence of a participant's permanent or temporary hired staff shall be attributed to the participant.

6.2 The **sanctions** that the board can impose on participants are: warning, suspension and exclusion. The Audit Committee may present the board with a recommendation supported by reasons why a certain sanction should be imposed on a participant.
6.3 Prior to the sanction being imposed, the board shall attempt to come to an agreement with the participant regarding an **amicable solution** for the existing problem. If achieving an amicable solution fails, the board may proceed to impose a sanction.

6.4 The **suspension** of a participant shall carry a certain period for the suspension. Such a period shall not be longer than six months. The suspension may be extended once by the same period by the board. If the suspension carries certain conditions that must be fulfilled or actions that must be performed, the suspension shall lapse as soon as the participant has demonstrated to the satisfaction of the board that he/she has fulfilled the conditions set or has performed the required actions. A suspension entails that, for the duration of the suspension, the participant shall not have access to the Warning Register for consultation or entering data.

During the period of suspension, the suspended participant's information obligation within the context of the retrieval procedure remains in force. Only access to the relevant fraud file is required for this purpose.

6.5 The **exclusion of a participant** shall only be imposed as a last resort if situation has arisen involving a participant's actions and/or negligence that are flagrantly in conflict with the Protocol for a longer period of time and repeatedly or in circumstances where the interests of the *Stichting FAD* and/or other participants have been severely damaged knowingly and willfully, or the integrity of the Warning Register has been brought into serious disrepute, or in the case of a participant who has already had one or more sanctions imposed.

6.6 If a decision has been made to exclude a participant, this participant shall immediately be denied access to and use of the Warning Register, in any form whatsoever. All the persons entered by the excluded participant shall be immediately deleted from the Warning Register because the excluded participant can no longer function as informant within the context of the retrieval procedure in response to the vacancy holding participant. Such cases likely involve on-going conflicts between the board and the ultimately excluded participant. Therefore, it does not make much sense to impose the obligation on the excluded participant in such a situation of handing his/her fraud files over to the FAD secretariat so that the information obligation could be exercised during the retrieval procedure. Such an obligation would probably lead to further discussions that would not benefit anyone.

7. The Warning Register

7.1 The Warning Register represents an **automated processing of personal data** within the meaning of the GDPR. The Warning Register meets the requirements of **proportionality** (no other personal data is processed than is strictly necessary) and **subsidiarity** (there is no other, less intrusive means available for achieving the intended aim). The Warning Register is **properly secured** by technical and organisational measures against hacking, data breaches and illegal processing of the personal data. A **data protection officer** has been appointed to supervise the proper functioning of the Warning Register within the context of protecting personal privacy. This person will fulfil the statutory duties referred to in Article 39 of the GDPR.

7.2 The **goal** of the Warning Register is to facilitate fraud protection for affiliated participants by offering them an instrument for registering personnel who have been dismissed due to internal fraud, and for integrity screening of applicants for jobs in the retail trade.

7.3 The participant or sector service association is authorised to **enter** a few personal details of an individual natural person from the incident register into the Warning Register if and after **all** the following **conditions** have been met:
a. the participant or an external expert hired by the participant has determined by means of a **careful examination** that the person has **committed an internal fraud**; and

b. that person has been **dismissed** due to the said internal fraud, or the employment relationship with that person has been terminated for the same reason; and

c. that person has been **reported** to the police as having committed a criminal offence and the police have made up an **official report** for that person.

7.4 For every internal fraud that leads to personal data being entered in the Warning Register a digital or paper file shall be kept with all the relevant documentation and evidence (**record-keeping requirement**) by the participant or the sector service association.

7.5 Only the following personal data shall be recorded in the Warning Register: sex, first name(s), last name prefix, last name, supplementary last name, date of birth, place of birth, search key, personnel id, file number, reasons for inclusion in the WR, dismissed (yes/no), reported to police (yes/no), date reported to police, number of report to police, period of retention, expiry date, status, registration date. Recording the BSN (c**itizen service number**) in the Warning Register is prohibited (Article 46, paragraph 1, GDPR Implementation Act).

7.6 A participant shall only proceed to enter personal data in the Register following a **weighing of interests**, whereby the interest of registering the data (protection of affiliated participants against employing persons who have already been dismissed for internal fraud) shall be weighed against the interest of the person involved not to be registered (**proportionality test**). All the relevant facts and circumstances of the case shall be taken into consideration when weighing the interests. The consequences of registration for the person involved must be proportionate to the seriousness and 9

scope of the internal fraud and the circumstances of the case. Even participants who maintain a strict integrity policy or zero tolerance policy in their businesses are always required to conduct a proper weighing of interests. In those cases, the participant's interest shall be heavily weighted since employees were already familiar with that policy.

7.7 Any other use of the data from the Warning Register for purposes other than assessing the integrity of job applicants in the context of a recruitment procedure (**pre-employment screening**) is prohibited.

7.8 If during an **integrity test** a person's name is found in the Warning Register (a so-called 'hit'), the participant with the job vacancy shall request information from the primary source (**retrieval obligation**). In fulfilling the request, in each case the identity of the designated person shall be verified, and in addition further information may be provided concerning the internal fraud. The participant with the vacancy shall always satisfy the retrieval obligation and shall decide about filling the vacancy following receipt of the information from the primary source.

7.9 Participants shall appoint one or more persons in their organisation who shall be authorised to take decisions regarding entering of information in the Warning Register, after conducting the proportionality test, to carry out the necessary actions to that end, and to screen job applicants using the Warning Register (**authorised persons**). Such authorised persons shall receive the necessary instructions from the participant on how to work with the Warning Register. They shall be bound by a **duty of confidentiality** for that which they come to know in their job, unless this concerns processing within the objectives of the Warning Register (feedback and information obligation).
7.10 Personal information shall be **deleted** from the Warning Register:
a. following expiry of the registration period;
b. if a request from a person involved for deletion has been granted;
c. on the instructions of the board, the Audit Committee, or the Complaints Committee.

8. The rights of the data subject

8.1 Participants' incident registers and the Warning Register are processes from which information shall be provided upon request to the data subject about the information about him/her entered into the Register or notification that the data subject has not been entered. The Protocol for the Warning Register shall be published on the website stichtingfad.nl, and may be downloaded. It can also be obtained from the secretariat of the *Stichting FAD* upon request.

8.2 The person who has been entered in the Warning Register on account of internal fraud shall receive a **written notification** of the fact and the period of entry in the Warning Register from the participant as soon as possible. This shall also explain the right of inspection and correction, and the possibility of lodging a complaint with the Complaint Committee.

8.3 The data subject can enforce his/her **legal rights** in respect of the Warning Register by contacting the *Stichting FAD*. The secretariat shall issue the data subject with information pertaining to his/her registration in the Warning Register, following proper identity verification based on a copy of a valid passport or a valid identity document.

8.4 If corrections or additions to, deletions from, or blocking of information pertaining to the data subject are made at the said person's request, the board is responsible for ensuring that the changes are communicated to participants who had received the information about the data subject before the change was made, unless this is impossible or requires a disproportionate amount of effort.

8.5 The data subject has the right to approach a participant for whom he/she worked with a request to find a reasonable solution, if in said person's opinion entry in the Register was unwarranted or the period of registration is too long. If the participant refuses to comply with the request of the data subject, the latter may approach the Complaints Committee with a complaint. The data subject has the right the right to apply to the competent court at any time.

9. Monitoring

9.1 An **Audit Committee** has been struck, which is the sole body authorised by the board to monitor compliance with the Protocol.

9.2 The Audit Committee shall consist of **at least three members** who are experts in the retail trade, privacy legislation, security and ICT fields. The members shall receive an honorarium as determined by the board for their activities.

9.3 The **tasks** of the Auditing Committee are:

a. monitoring compliance with the Protocol by conducting **audits** among the participants, reporting the results to the participant and the board, as well as issuing binding instructions for the participant's improvement;

b. acting as contact point in cases of a data breach and taking urgent measures, or have them taken on its behalf, to prevent further damage or harm, as well as submitting proposals to the board on how to improve security around the Warning Register, and reporting data breaches to the Dutch Data Protection Authority, should such a report be required;

c. having personal data deleted from the Warning Register if this data has been wrongfully entered or wrongfully left in when it should have been deleted;

d. issuing an annual report to the board covering its work and, where necessary, making proposals to the board for improvements to the Warning Register based on the findings of audits conducted.

9.4 The Audit Committee may make **recommendations** to the board, if findings based on its tasks prompt such action.

9.5 The Audit Committee shall be bound by **regulations** that are determined by the board. The Committee is authorised to further organise its activities as it sees fit supplementary to the regulations.

10. Complaint handling

10.1 There is an independent Complaints Committee, which is charged with the careful processing of complaints from persons who have been entered in the Warning Register and whose attempts to find an amicable resolution to the problem with the participant have been in vain.

10.2 The Complaints Committee shall consist of three members: a lawyer as chair, a lawyer as rapporteur, and a member drawn from the pool of participants. The members shall receive an honorarium as determined by the board for their activities.

10.3 The Complaints Committee shall issue a **binding judgment** following processing of the complaint. The board shall receive a copy of every judgment. The Complaints Committee is authorised to have the personal data of the appellant deleted from the Warning Register, if this data has been wrongfully entered or wrongfully left in when it should have been deleted. The Complaints Committee is further authorised to suspend or shorten the period of registration.

10.4 The Complaints Committee may make **recommendations** to the board, if findings based on processing a complaint prompt such action.

10.5 The Complaints Committee shall be bound by **regulations** that are determined by the board. The Committee is authorised to further organise its activities as it sees fit supplementary to the regulations.

11. Amendments to the Protocol

The board may decide to amend the Protocol and/or the accompanying Notes. Before implementing an amendment, the board shall **consult** with **the participants** and offer them the opportunity to communicate their wishes or objections. After careful consideration of the participants' comments, the board shall ratify the amendment. The Protocol and Commentary are **binding for the participants** following ratification of the amendment.
Name and position (signed exclusively by the director under the articles of association)

Signature:
Participant's name:
Signed in: **on:**
Name and position: ***(signed exclusively by the director under the articles of association)***
Signature:

CONTACT
Visiting address
Overgoo 13
2266 JZ Leidschendam

MAILING ADDRESS
Box 182
2260 AD Leidschendam
Telephone (070) 444 25 87

info@stichtingfad.nl
www.stichtingfad.nl

FAD
Fraude Aanpak Detailhandel