Notes to the FAD Protocol (Version 4.0)

The phenomenon of internal fraud

An employer's trust in his staff is central to any employment contract, because without this trust, no employer can successfully run its company. Employees are what form the main capital and are what 'carry' the company. In addition, many businesspeople call on the services of hired staff in order to save costs and ensure efficiency. What's more, companies act as work placement provider for students taking courses that focus on the retail trade, and they facilitate major participants in the sale of special products in their stores by third parties, who often use their own employees for this (*shop-in-shop formula*). This extremely varied overview of staff determines how a company will actually perform.

Breach of trust

A fraud committed within an affiliated retail company by the company's own or a hired member of staff constitutes in all cases a serious breach of trust in the existing employment relationship. The business is effectively being robbed, scammed and taken advantage of 'from the inside' by one of its own members of staff. The discovery of an internal fraud will naturally hit employers hard. The trust that the employer thought it was able to place in the person concerned has been violated. What's more, an internal fraud has a negative impact on the atmosphere at work and could send the wrong signal to other members of staff. This is why it makes perfect sense and is entirely appropriate that many participants within their company take measures to discover internal fraud and to make it more difficult for perpetrators to commit, as well as to pursue a targeted policy to encourage honourable behaviour and to actively fight internal fraud. In addition, cases of internal fraud often give rise to changes to processes and procedures within the company in order to make internal frauds even more difficult or impossible in the future.

From internal fraud to criminal offence

Internal fraud is an *actual concept* which, as such, does not have any criminal significance. An internal fraud generally consists of an action or actions (or a combination thereof) which individually or together constitute a *criminal offence*. In most cases, it concerns: theft, embezzlement (in employment), scams, forgery of documents etc. Each internal fraud can therefore be 'translated' into a criminal offence (or suspicion thereof), which in turn can be reported to the police. The data subject may only be entered in the Warning Register (*Waarschuwingsregister*) once the report has been filed by the police and recorded in a statement, combined with other requirements.

Three requirements for registration

A decision to register an employee in the Warning Register may only be taken if the following three requirements have been met:

1. It must be possible to establish sufficiently that the data subject has committed internal fraud on the basis of a stringent investigation; and
2. the data subject must have been discharged or the employment relationship terminated on the grounds of this fraud (with respect to temporary staff); and
3. a report against the data subject must have been filed with the police.

This concerns the *sum of three requirements* and all three must have been met (*cumulative requirements*). If one of these requirements has not been met, the data subject may not be registered in the Warning Register.

Stringent investigation

An investigation into suspected internal fraud will either be conducted internally, by employees of the company themselves, or by an external security agency which has been brought in for that purpose. The major players have their own Security and Loss department, which is able to further investigate suspected internal fraud. Each investigation will need to be stringently conducted. In addition, hidden cameras may only be used if there is no other effective, less intrusive way available of proving internal fraud. In order to prove fraudulent cash register transactions, a hidden camera installed in the cash register area of a shop, combined with cash register overviews and built-in technical facilities, will usually be the only effective method. An external security agency that has been brought in may be required to carry out its work on the basis of a *code of conduct* which is generally applicable in the *security sector* (*state of the art*). The results of the investigation must be laid down in a report. A stringent investigation includes an *interview* between the researcher and the employee concerned in which the employee accounts for his/her actions. The data subject must be notified of the purpose of the interview when invited to interview. In this interview, the data subject will be confronted with the findings of the investigation. *Minors* must be heard in the presence of a parent or guardian, unless they expressly say that they do not wish for them to be present. The data subject must be given the opportunity to give his/her view on the conclusions of the investigation. An *additional investigation* must take place if necessary if the response of the data subject gives cause for this to happen. The data subject should not have to face a 'tribunal' of employees from the company, as this could be considered imposing. It is recommended that a branch or regional manager is present in addition to the investigator, as he/she will be aware of how things work in his branch or region. During the interview in which the employee accounts for his/her actions, the data subject must not be pressured into signing a (pre-drafted) *statement of confession*. Any statement made by the data subject must be made voluntarily. In order to achieve that, it is preferable that the data subject is allowed to formulate his/her own confessions. In the given circumstances, that alone is often already difficult enough. A stringently conducted interview concludes in an *accurate report* of what has been discussed and agreed.

Dismissal, termination of employment relationship

During the meeting with the data subject, *notice may be given* of a recommendation for dismissal or a dismissal on the grounds of gross misconduct ('with immediate effect'), provided that the individual who gives the notice within the company is authorised to do so. The notice given during the interview must then be confirmed to the data subject in writing. It is recommended that the *letter of dismissal* is sent by both registered and regular post to the home address of the data subject, in order to prevent any problems concerning its receipt. Dismissal on the grounds of gross misconduct is not required. Any dismissal on account of internal fraud is sufficient to meet the dismissal requirement. In the case of hired staff, the *employment relationship* must be *terminated* early. In that case too, the identified fraud will have to be used as grounds for dismissal.

Reporting of a criminal offence

In the case of an internal fraud that has been established to a satisfactory extent following an investigation, one or more criminal offences (or the suspicion thereof) will always be involved. The data subject must be reported to the police for this offence and this report must actually have been recorded and laid down in writing.

Record-keeping requirement

For each specific case of internal fraud that has led to the registration of the data subject in the Warning Register, the participant must compile a file and retain it for later reference. This can either be in the form of *a hard copy or a digital file*. The file must have all relevant documents available for later investigation by the Audit Committee or the handling of a complaint by the Complaints Committee. It must therefore be possible to verify each registration in the Warning Register in a *fraud file* that is in the participant's possession. The record-keeping requirement applies for the duration of the registration, in other words 2 or 4 years. If, when a random check is carried out or a complaint is being handled, no grounds for the registration is found in an underlying file, the registration in question will be removed. Guaranteeing the integrity of the Warning Register requires a transparent decision-making process which can be traced later on in relation to each registration.

The Protocol contains a number of provisions in relation to the *record-keeping requirement in special cases*. These must continue the record-keeping requirement, even after the participation has ended, or following liquidation or another form of cessation of business activities. Even afterwards, all current registrations must be supported by an underlying file for their duration. If that is not possible, the registrations of the data subjects that have been included by the participant in question will be removed. In order to prevent this latter situation, fraud files for which no other acceptable storage place is available will be transferred to the secretariat of the Foundation for Fraud Prevention in the Retail Trade (*Stichting FAD*), which will then act as registering participant (primary source) in the context of the retrieval procedure.

Personnel consequences of an internal fraud

An internal fraud generally has serious consequences for the employee concerned. In many cases, certainly in the companies of the participants where an integrity policy applies, an internal fraud is usually followed by a dismissal on the grounds of gross misconduct ('with immediate effect'). In addition, the decision is generally taken to enter the fraudster in the Warning Register. An internal fraud therefore has both *legal consequences* (dismissal, criminal prosecution) and *consequences for the employment market* (registration). The data subject will encounter problems when looking for alternative work in the retail sector, especially among other participants. These aspects are separate from each other, but do amplify each other in terms of the consequences encountered by the fraudster. Yet it must be possible to easily differentiate between the consequences of a fraud.The following overview can be used for that purpose.

Employment law

A dismissal granted on the grounds of internal fraud may be contested by the data subject in employment law proceedings at the subdistrict court. Only a court judgement that has wrongfully granted the dismissal because there were insufficient grounds to do so (for example, insufficient proof of the internal fraud), will have consequences for the Warning Register. With this court judgement, one of the three pillars falls away under the registration (the internal fraud has been identified on the grounds of a stringent investigation), with the result that the registration cannot be maintained and must be deleted. All other judgements in employment law proceedings are of no importance to registration in the Warning Register.

Criminal law

The Public Prosecution Service (public prosecutor) may decide to prosecute on the grounds of the report of a criminal offence against the data subject. The data subject must then justify the suspicion of one (or more) punishable act(s) to the police court in criminal proceedings. A common misconception is that an acquittal or dismissal of judicial persecution in criminal proceedings must also lead to removal of the data subject's registration from the Warning Register. That is not the case. Higher requirements are placed on criminal evidence than on identifying internal fraud following a stringent investigation conducted or commissioned by a participant. The fact that the court rules that there is no legal and compelling evidence of a criminal offence committed by a suspect does not therefore have any consequences for his registration in the Warning Register. That is and remains based on the internal investigation carried out on the participant.

Employment market

The only consequence upon which the Warning Register focuses is warning other participants against a previous internal fraud committed by an applicant to a job in the retail sector. In the employment market, a registered fraudster will therefore encounter problems when applying for a job in the retail sector with an affiliated participant. When the return of money is ordered after a fraudster has had a 'hit', aspects such as the identity of the identified fraudster, and other details, will be verified, in order to prevent a case of mistaken identity. Of course, a participant may decide to employ a fraudster despite a 'hit', because he/she has the required experience and/or expertise (e.g. specific knowledge of the sector), for example. It is up to the participant to decide what consequences he attaches to a 'hit'. Entry in the Warning Register therefore does *not mean an employment ban for the retail sector*. The employment market as a whole is also much broader than the retail sector, which means that a fraudster registered in the Warning Register has plenty of opportunities to find work outside of the retail sector.

Deliberate relinquishment of registration

In exceptional cases, there may be reason not to register an internal fraudster in the Warning Register. A registration may be relinquished due to stringent personnel policy or on the grounds of the exceptional circumstances of a specific case. The decision to do so is up to the participant, as is the case with a major participant who has relinquished registration of an employee who was the victim of a lover boy and who had been pressured by him to steal items 'to order'. The employee was dismissed at the time, but was not entered in the Warning Register. The lover boy was reported rather than the employee. This example shows that these are very exceptional circumstances in which the question is whether the committed internal fraud is sufficiently culpable and whether

inclusion in the Warning Register is not a disproportionately incriminating measure for the data subject. This concerns customised solutions in exceptional cases and in the context of the personnel policy of the participant. In that case, there may be reason to apply the principle of 'tempering justice with mercy'.

Consequences of internal fraud for a work placement student

In the context of an senior secondary vocational education course (*mbo-opleiding*) or a university of applied sciences degree programme (hbo-opleiding) study programme focusing on the retail sector, students undertake work placements with the various participants. Successfully passing a work placement such as this is a requirement for obtaining the diploma for these retail sector study programmes. A work placement student could potentially commit internal fraud during his/her work placement. These are not generally serious cases of fraud that would justify a 4-year registration in the Warning Register. In such a case, the consequences of a registration in the Warning Register are disproportionate: the data subject is shown the door by the participant providing the work placement, so he/she is unable to complete his work placement and will find it difficult to be accepted by other participants as a work placement student either. As a result, the data subject will be unable to complete his/her work placement, which essentially equates to an employment ban in the retail sector.

A serious consequence of a one-off and relatively minor offence such as this is disproportionately harsh for the data subject. The Complaints Committee has made an arrangement for such - therefore not for all - cases that makes it possible for the data subject in the context of a complaint to request suspension of the registration until the moment that the diploma of the retail sector study programme has been obtained or this study programme has otherwise been terminated by the student. An arrangement made with the educational institution will ensure that the *Stichting FAD* is notified of the outcome of the study programme for the data subject. From that moment on, the registration will be restarted and the data subject will still have to face the consequences of the registration on the employment market, but as a qualified member of retail sector staff. During the suspension, the data subject then has the opportunity, seemingly with a 'clean slate', to find another company in the retail sector as a work placement provider and still to meet the work placement requirement of the study programme. The participant company where the fraud occurs during the work placement is excluded from this specific arrangement. The participant may therefore end the work placement early on the grounds of fraud and enter the data subject in the Warning Register after the proportionality test has been taken. This concerns a *goodwill arrangement* by the independent Complaints Committee. The Protocol therefore does not report anything about this and the participant who has sent the work placement student away following the internal fraud is not covered by this.

Deliberate policy for combating internal fraud

Many participants pursue a deliberate policy within their company to combat internal fraud under names such as: integrity policy, zero tolerance policy etc. A consensus has been reached with the (central) works council in relation to such a policy, management is actively implementing that policy and when they commence their employment, new employees receive the text for the applicable policy as an annex to their employment contract, which also legally binds them to comply with such

policy rules. These rules are therefore generally known among staff within the company where they apply. As a result, each employee can be considered a 'warned person'.

The validity of such a policy may therefore count as an aggravating element when carrying out the proportionality test. After all, the member of staff knew that failure to act honourably (committing internal fraud) will not be tolerated and will be severely punished (generally with 'immediate dismissal'). However, it is going too far to determine in such policy guidelines that an identified case of internal fraud will be followed by reporting and recording in the Warning Register for 4 years at all times. An automatic process is thereby being introduced that is not compatible with *the essence of the proportionality test*: making a motivated choice to be included in the Warning Register and for the appropriate registration period in a specific case of internal fraud on the grounds of a careful consideration of all the relevant facts and circumstances. For each case, a decision will therefore have to be taken here too with regard to whether or not to include in the Warning Register and with regard to the registration period. If the decision is taken to enter the case in the Register, which decision will incidentally be more the rule than the exception, the period for which the fraudster will be entered in the Warning Register will therefore have to be tested on a case-by-case basis. Due to a participant's general familiarity with applicable integrity rules, he/she may be more likely to choose a period of 4 years, but not necessarily in all cases. For example, when an internal fraud has been committed, a manager (setting an example) who has worked for the company for many years (loyalty to the company) and a limited loss amount will be more likely to qualify for a period of 4 years, whereas for a young part-time weekend assistant with the same loss amount, a period of 2 years is appropriate. The consideration of the registration period (2 or 4 years) must form part of the case file and may be assessed by the auditor during an audit. The Complaints Committee may also cover this aspect in its investigation.

Solidarity: giving and taking, supplementing and consulting

The Warning Register is based on the *mutual solidarity* of participants in the retail sector. They use the register to warn each other about bad experiences with internal fraudsters who previously worked for one of the participants. When applying for jobs with other participants in the retail sector, the data subject will then be flagged up by the register as a fraudster. The participant with the vacancy to whom an application has been made can then partly base his decision as to whether or not to employ the data subject on the information provided about this individual. As part of the *retrieval procedure,* further information about the details of the fraud can be obtained from the aforementioned employer if required. After all, a (hard copy or digital) fraud file is available for each internal fraud resulting in inclusion of the data subject in the Warning Register, from which a complete overview can be requested of what occurred during the deliberate internal fraud.

There are two consequences to the solidarity between participants forming the basis for the Warning Register, namely:

1. Each participant must be willing, as far as possible, to file a report after each case of internal fraud; after all, without a report, it is not possible to enter fraudsters in the Warning Register;
2. Each participant must play his/her part in adding to the Warning Register; the main purpose of affiliation as a participant should not be to consult the register as an additional selection tool in applications.

Here it's more a case of 'you scratch my back and I'll scratch yours'. It's all about give and take: adding to and consulting the Warning Register.

A Warning Register to which new fraudsters are actively being added by the participants is not just a valuable way of protecting other participants in the retail trade against employing the data subjects. The Register also provides an almost complete insight into the scale of the internal fraud by the company's own or hired staff among all participants. Each year, the relevant basic information concerning internal fraud in affiliated retail sector companies and the trends and developments are published in the *Stichting FAD's* annual report, giving the nature and scale of the phenomenon of internal fraud the social significance and attention that is unfortunately required.

Willingness to file a report

The *willingness of participants to file a report* is one of the core values of the Warning Register. After all, without a report, the case cannot be registered in the Warning Register. As a result, the value of the Warning Register as a source of information when taking decisions about whether or not to employ applicants reduces. It is not always easy for the participant to actually file a report: limited availability of the reporting officer or other priorities among the police can make it more difficult to file a report. Yet the basic principle remains: *no report, no registration*. The same will apply in the future too. The Retail Crime Platform (*Platform Winkelcriminaliteit*) repeatedly asks the retail sector to pay attention to the *practical problems* encountered by participants *when filing a report with the police*. Excess shortages of police staff and other investigation priorities prevent a quick solution to this problem from being found. Some participants in a number of cases have made fixed arrangements with the police in their region with regard to an efficient procedure for reporting internal fraud. The board of *Stichting FAD* has been able to make arrangements with the Leidschendam-Voorburg police unit with regard to the recording of reports made by participants encountering problems when filing reports. They can still file a report via the secretariat of *Stichting FAD* in Leidschendam and obtain a record of the report, and then the fraudster in question can be entered in the Warning Register. A pilot is currently (2020) underway in which this reporting route is limited to SME retailers affiliated with a branch office. Following an evaluation of the practical experience, this reporting route may also be made available to other participants. If the decision is taken to make this available, a general safety net will be present for all participants to gain quick access to a record of the report if they encounter practical obstacles to filing a report at their own regional police unit.

Proportionality test

When dealing with a case of internal fraud involving the potential entry of the fraudster in the Warning Register, the so-called *proportionality test* is discussed. This encompasses *two aspects* ('two-stage rocket').

The *first question is whether the fraudster must be entered in the Warning Register*. This question will generally be answered in the affirmative due to the significant importance of protecting the retail trade against internal fraud. Yet staff policy may consider not including the data subject in the Warning Register, given who the perpetrator is and/or the particular circumstances of the case. In such a case, a severe '*final warning*' can be given. When considering this matter, all relevant aspects of the case must be taken into account. It may also become apparent that entry in the Warning

Register would mean too severe a sanction for this individual under these particular circumstances. These are exceptions to the general rule that follows for participants based on their affiliation with the Warning Register, namely: to enter in the Register as far as possible.

Then, if the first question is answered in the affirmative, the *second question* is discussed, namely *what sanction (registration for how many years) is appropriate for the identified fraud*. This must have been established on the basis of an in-depth investigation which gave a complete picture of the fraudulent acts of the data subject(s) and the circumstances under which they committed the fraud. Many and different factors also play a role, the main ones being: the character traits of the data subject, the nature and scale of the fraud and the circumstances under which the fraud was committed. Internal fraud occurs in many different forms and the severity differs from case to case. When it comes to the proportionality test that is to be carried out, this is why it must be considered whether 2 or 4 years is the appropriate period for registering the fraudster on a case-by-case basis. It cannot be said exactly where the tipping point between these two periods lies, but it is important to bear in mind at all times that entry in the Register for 4 years is the most severe sanction possible, so it is only appropriate for severe cases of fraud. Therefore, it is not permitted to register individuals for 4 years in all cases on the grounds of an active integrity policy or zero tolerance policy that applies to a participant. After all, such an approach actually means that a proportionality test is not being carried out, because individuals are always being registered for the longest period. That is contrary to the essence of the proportionality test, which includes a well-reasoned decision as to whether or not to enter someone in the Register and whether the registration should be 2 or 4 years in duration. Any automatic process, in whatever form, is not in keeping with this.

Consideration of all relevant aspects

In the context of the proportionality test, all relevant aspects of the data subject and the internal fraud must be taken into consideration and form part of the decision as to whether or not to include an individual in the Register and a suitable period. It concerns factors such as: age, term of employment contract, job title, nature of the fraud, number, frequency and duration of fraudulent acts, collusion with others, position as initiator or follower in this, loss amount (loss), manipulation of cash register system, measures taken to prevent discovery, whether the person is a line manager, whether the person works with money, abuse of power (e.g. awarding of staff discount, giving preference to acquaintances), ignoring of orders given by managers, violation of applicable company regulations (e.g. zero tolerance policy).

Point of reference: 4-year registration is exceptional

In order to make the decision easier, the following general outline of an internal fraud for which a 4-year registration period is appropriate can be used as a reference point. In this case, there will generally be a combination of factors such as: manager (setting an example), long duration of the fraud, large loss amount, sophisticated way of working (manipulation of systems to prevent discovery), initiator in joint fraud (domino effect), serious deterioration of the positive working atmosphere, others wrongfully suspected, valid zero tolerance policy, external consequences (negative publicity, damage to reputation), theft of colleagues' property etc.

If, in a specific case, there is no evidence of the aforementioned factors (or a combination thereof), a 2-year period is usually appropriate. With this approach, a 2-year registration is more likely to be

deemed appropriate than a 4-year registration. In other words: based on the picture of the registered internal frauds over the past years, a 4-year registration would have to be rather exceptional.

Audit Committee

The Audit Committee plays an important role in guaranteeing the integrity of the Warning Register based on the FAD Protocol and the Notes to this Protocol. It is the only body authorised to monitor compliance with the Protocol and/or the GDPR within the participant's organisation by order of the board of *Stichting FAD*. So during an *audit,* the actual way of working with the Warning Register is mapped out and it is assessed whether this way of working is in accordance with the Protocol and applicable privacy legislation. Audits may be carried out on a participant, but also on the processor or the controller. The Audit Committee also has an *advisory function*, especially for employees of newly affiliated participants. An initial audit usually takes place during the first year of affiliation. For each audit, recommendations may be given in relation to shortcomings and tips for improvement. A *report* of each audit is drawn up, which is presented to the visited participant in draft format. This participant then has the opportunity to comment on the Audit Committee's findings and conclusions. Attempts will be made at all times to reach agreements with the audited participant that deliver a way of working that is in accordance with the Protocol and/or GDPR. By processing the comments of the audited participant and through any agreements reached with regard to improvements, the Audit Committee draws up the final report of the audit. If the Audit Committee is unable to reach an agreement with a participant in relation to practical improvements, the audit report may be brought to the notice of the board of *Stichting FAD*. In any case, there is cause to do so if the Audit Committee proposes that the board imposes a sanction. The Audit Committee issues a report of its activities to the board every year.

Sanction policy

The Audit Committee acts as the eyes and ears of the board. Carrying out audits among the participants provides insight into day-to-day practice when working with the Warning Register. In addition, shortcomings may become apparent that need to be rectified by the audited participant. A solution will generally be reached in close consultation between the auditor and the participant/the participant's staff. However, we have learnt from experience that this is not always the case. A whole host of circumstances (such as insufficient priority, staff changes, reorganisation) means that no or insufficient measures are being taken to bring the practice at an audited participant into agreement with the Protocol and/or GDPR. Such cases, even if a *second audit* fails to yield a solution, are reported by the Audit Committee to the board, which is responsible for the integrity of the Warning Register. The participant's failure to act jeopardises this integrity. This is why the new article 6.1 of the Protocol gives the board the power to impose a sanction on the negligent participant. This participant will be notified of the board's intention to impose a sanction on him/her and he/she will be given an opportunity to rectify the identified shortcomings within a reasonable period of time. If the participant's actions to rectify the matter from or his measures for improvement remain unsatisfactory, the board may decide to impose the sanction. Depending on the nature, severity and duration of the shortcoming, the decision may be taken to impose a more or less stringent sanction. Even after the sanction has been imposed, the participant will still be required to take appropriate measures, unless he is excluded from further participation in the FAD or is terminating his

participation. The other participants will be notified of the imposition of a suspension or exclusion. However, that is not necessary in the case of a warning, because in that case, no situation has occurred that can be carried over to other participants. After all, a warning focuses on the prevention of repetition of an undesirable situation that has already been resolved or the cessation of existing shortcomings in order to prevent the further and more stringent imposition of sanctions. This stringent procedure makes the imposition of a sanction a *last resort* once it has become apparent that the participant is twice unwilling or unable to rectify the identified shortcomings. An internal authority that has the authority to impose sanctions is vital for protecting the integrity of the Warning Register, also partly in light of the authority of the *Dutch Data Protection Authority* to impose *fines*.

Data Breaches (Reporting Obligation) Act (*Wet meldplicht datalekken*)

Part of the task of the Audit Committee is to investigate reports as referred to in the *Data Breaches (Reporting Obligation) Act* (article 14, paragraph 1, in conjunction with article 13) and, based on its findings from that investigation, to take (or have taken) the necessary or most appropriate measures, including a report to the Dutch Data Protection Authority (article 34a, paragraph 1). The Audit Committee also provides the *documentation* for all data breaches (facts, consequences and corrective measures taken) which have arisen in the Warning Register. The Audit Committee carries out this work on the basis of a permanent authorisation of the board as the person responsible (article 14, paragraph 3). The Audit Committee notifies the board about its activities and acts in the context of the Data Breaches (Reporting Obligation) Act in a specific case, as well as into relation to data leak documentation.

Legal position of the data subject

As the data subject, the person about whom details have been included in the Warning Register has the rights granted to him by the GDPR and the GDPR Implementation Act (*Uitvoeringswet AVG*). The participant for whom he worked will notify him in writing of the fact that he will be entered in the Warning Register. He/she may then ask that participant for a report or statement of the details held about him in the Warning Register or to notify him/her until if he/she has been registered or request for his/her details to be removed, because these disproportionately hinder him/her in seeking alternative work or his registration is disproportionately damaging for other reasons. It will take some time for a participant to meet such a request, because during the proportionality test, all relevant factors, including the aspects that concern the data subject, have already been weighed up against the interests of the participant. It is also important to realise that an entry in the Warning Register does not cause a situation in which it is impossible to find new work in the (affiliated) retail sector. After all, participants always take their own decisions in relation to whether to employ a job applicant who delivers a ‘hit’. They are able to see reasons still to employ the data subject, bypassing his/her registration. This is expected to remain limited to exceptional cases. As the final piece of the legal protection of the data subject, the Protocol provides a complaints procedure with an independent Complaints Committee.

Complaints Committee

The Complaints Committee is an *independent committee* that handles complaints made by the data subjects against their registration in the Warning Register. A complaint will only be handled by this

committee once the data subject has contacted the participant (the ex-employer) with the request for a solution and the participant has refused to meet the request of the data subject. This is the *admissibility requirement*. The data subject must prove with written documents that he was unsuccessful in contacting the participant. It is sufficient that the request is discussed and rejected by e-mail.

Complaints procedure

When the complaint is being handled by the committee, the committee asks the participant about whom the complaint is being made, known as the 'accused' in the complaints procedure, and for all documents relating to the case, as well as a written statement about the complaint. The complainant, known in the complaints procedure as the 'appellant', is given a copy of the complete file. During the procedure as a whole, the committee notifies the appellant of all developments in the handling of the complaint and he/she may submit a response to this if desired. If camera images of the internal fraud play a role in the handling of the complaint and the committee decides to view these images, the appellant will also be given the opportunity to view these images and to comment on them. The entire procedure is therefore characterised as '*a fair hearing'* and is transparent for both parties. Once all arguments have been shared between the parties, the committee closes the investigation and prepares a *binding decision*. A complete proportionality test is included in the decision at all times, in other words the committee gives its own opinion on the registration and the duration thereof based on all aspects that are to be taken into account. Once the decision has been made, it will be sent to both parties. In the decision, the complaint will be declared – entirely or partially – founded or unfounded and the committee may also decide to suspend the registration of the data subject (goodwill arrangement), reduce it to 2 years or delete it. A decision made by the Complaints Committee is also binding for the board of the *Stichting FAD* and is therefore implemented at all times.

Composition

The Complaints Committee consists of: two legal experts who are experts in privacy legislation (including the chairperson), as well as an expert from the retail sector. The latter is chosen from a *pool of participants* of people who work or have worked for one of the participants. The expert who participates in the complaint handling must not be connected or have been connected to the participant to whom the complaint relates. This guarantees that the complaint is handled in an expert and independent manner, contributing to the legal position of the data subject and guaranteeing the integrity of the Warning Register.

Amendment to the General Data Protection Regulation

EU Regulation the *General Data Protection Regulation (GDPR)* entered into force on 25 May 2018. This is having an immediate effect in all Member States of the European Union and has replaced the Personal Data Protection Act (*Wet bescherming persoonsgegevens*, Wbp) in the Netherlands. Since the aforementioned date, the GDPR is thereby the legal interpretive document for processing personal data. In the text of the Protocol, the terminology corresponds to the new legal framework of the GDPR/The Protocol is therefore 'GDPR-proof'. However, the decision has been taken to use

the generally accepted term ‘registration’ in the Notes where necessary, instead of the less well-known legal term ‘processing’.

Register (P refers to the Protocol (article), N to the Notes (page))