



DATA BREACH PROTOCOL FOR EMPLOYEES OF DÜMMEN ORANGE

1. INTRODUCTION

- 1.1 On the basis of the General Data Protection Regulation strict rules apply to Dümmen Orange as regards dealing with and processing security incidents such as data breaches. The regulator (the Dutch Data Protection Authority [Autoriteit Persoonsgegevens] (AP)) can impose extremely high penalties on Dümmen Orange if these rules are violated. It is therefore very important that if you, as a Dümmen Orange employee, identify or suspect any possible security incident, you report this immediately to the Data Breach Hotline and follow the procedure described in this protocol. Speed is of the essence in this respect because Dümmen Orange is obliged to process data breaches within 72 hours.
- 1.2 This protocol offers guidelines for the assessment and processing of security incidents and describes how you, as an employee of Dümmen Orange, should act in the event of a security incident, or if a security incident is suspected (the '**Data Breach Protocol**').

2. WHAT IS A DATA BREACH?

- 2.1 A data breach is a security incident where personal data is lost, or where unauthorised third parties have access, or can obtain access, to personal data (a '**Data Breach**'). Examples are server hacks whereby data is 'stolen', the loss of passwords which provide access to a data file, the opening of emails with viruses, the leaving, losing or stealing of portable media such as laptops, telephones or USB sticks and/or the forwarding of personal data to a person or organisation which should not have received said data.

3. OBSERVATION OF A (POSSIBLE) SECURITY INCIDENT BY AN EMPLOYEE

- 3.1 If you, as an employee of Dümmen Orange, suspect that a security incident may have taken place, or if you have observed a (possible) security incident, you must report this incident **immediately**, including all relevant information about the (possible) incident, by email to:

Data Breach Hotline

E-mail: Privacy@DummenOrange.com

You should also contact the Data Breach Hotline if you have any doubts.

for you



3.2 The information you provide to the Data Breach Hotline must include as many relevant details as possible about:

- the nature of the security incident and the actual circumstances insofar as known or suspected;
- the (possibly) affected personal data; and,
- (possibly) a proposal for measures to resolve or limit the (possible) security incident.

Keep this information in a safe place and make sure that it remains available for consultation by the Data Breach Hotline as long as is necessary for the processing of the security incident.

3.3 Incidents must be reported exclusively to the Data Breach Hotline. It is not permitted to issue (any) information about the (possible) incident to third parties, or to communicate with, or notify, the Dutch Data Protection Authority, the data subjects, or any third party with regard to the security incident. Dümmen Orange assumes that you will observe strict confidentiality with regard to the incident.

3.4 The Data Breach Hotline will process your notification and arrange the further processing of the incident.

for you