Authorisation types

Authorisation control allows the targeted allocation of various access authorisations, for example to certain forms, information functions, evaluation lists, etc. For example, it is possible to control that certain forms can only be accessed by certain employees or certain groups, or that an action such as booking or calendar is accessible to all employees.

The following **authorisation types** can be found in the action permissions:

Client permission	**Group permission**
Personal permission	**Role permission**

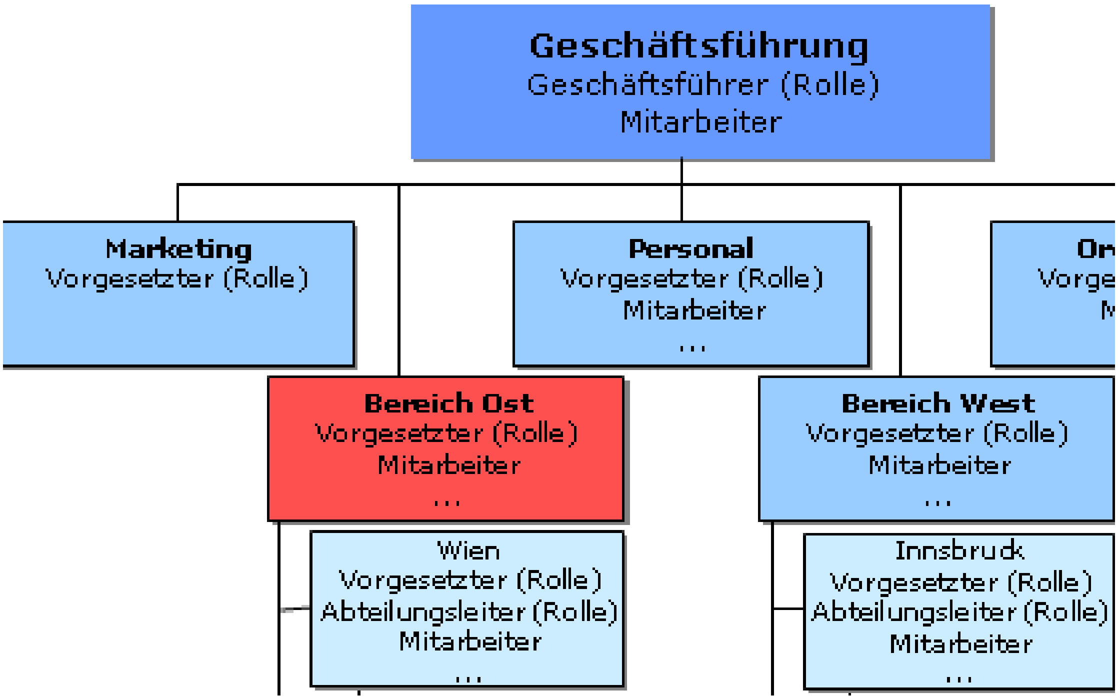
Authorisation is assigned either via the respective action, in the person master data sheet or via the role.

Client permission

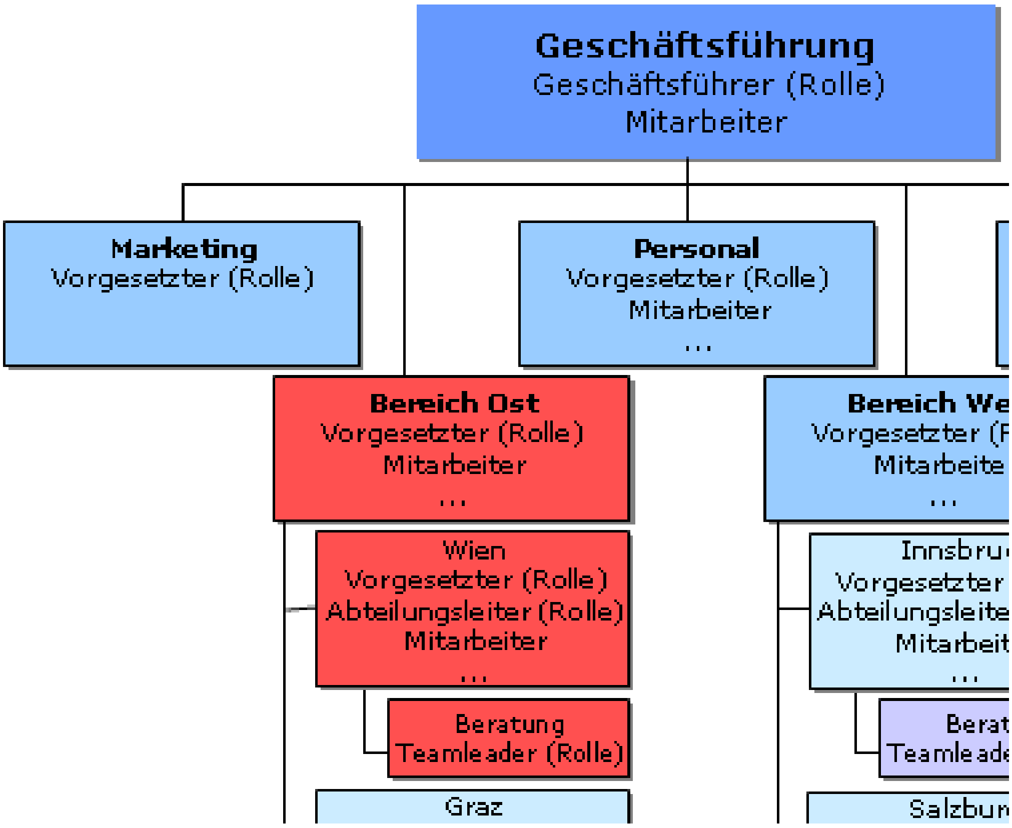
Client permission enables the execution of various actions for all employees of the client. This is particularly useful for actions such as booking, monthly journal, personal settings or changing passwords.

Group permission

Group permission enables the execution of various actions for a specific group (department). The following example shows a group authorisation for the "Bereich Ost" group (marked in red).

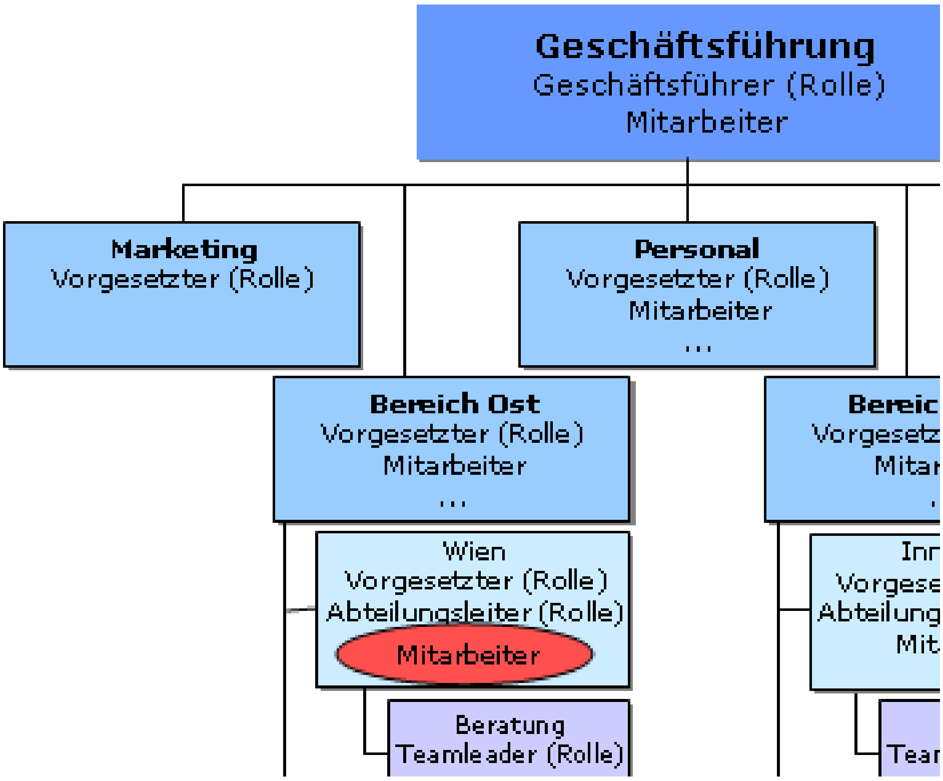


It is also possible to extend the group authorisation to the subordinate groups. This gives the subgroups the same access authorisation as the parent group. In our example, the groups "Vienna" and "Consultancy" are therefore also highlighted in red, as these are subgroups of the group "Area East".



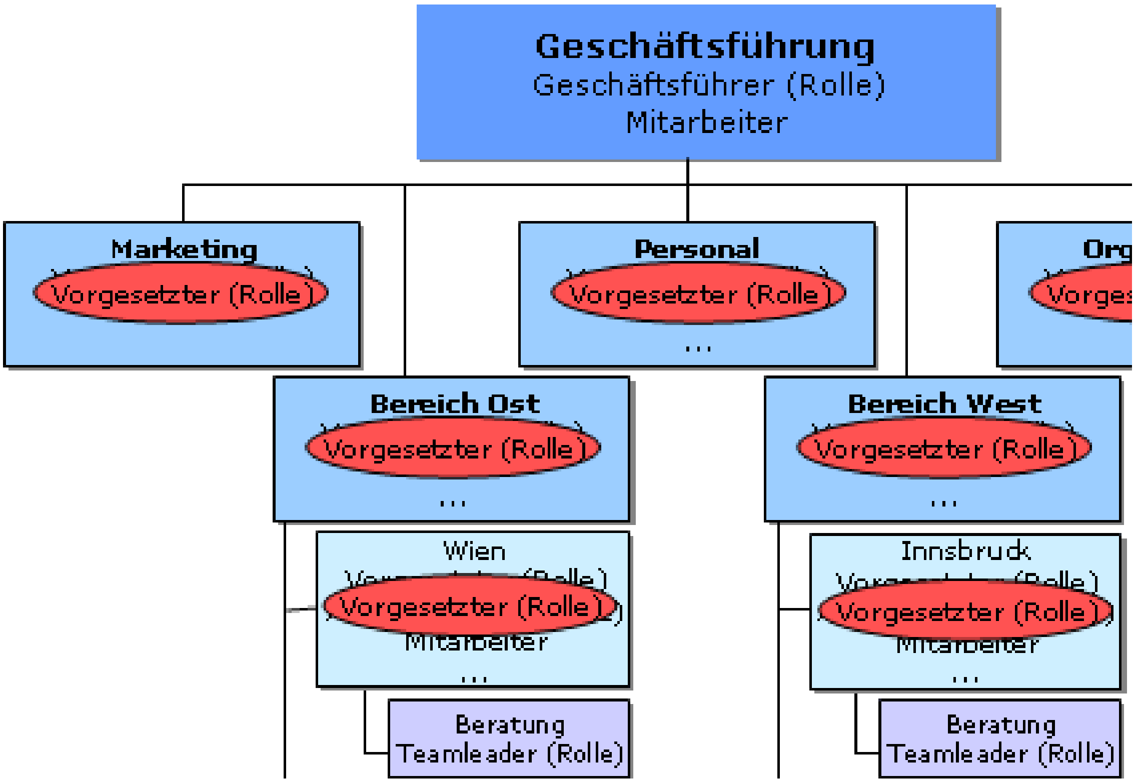
Personal permission

The person authorisation makes it possible to grant specific persons execution authorisation for certain actions.



Role permission

The role authorisation allows the execution of various actions only for certain role owners (team leader, supervisor, ...). This authorisation enables role holders to view management lists, for example. All role holders of the selected role in the organisation therefore receive the role authorisation and viewing permission (in accordance with the role competence defined in the role itself > competence target All, person or group).



Processing logic for authorisations

If an authorisation is given, the action or configuration for which the authorisation exists can be accessed. If the parent action is assigned in the menu tree instead of the action configuration and the current user only has explicit authorisation for a derived action configuration, they will still be forwarded to the appropriate action configuration.

If an action is implemented with several configurations in the menu tree (e.g. several variants of the monthly journal that are intended for different employee groups), the calculation of access or their configurations is carried out in a specific order.

Sequence of authorisation processing

The system first checks whether the authorisation is assigned to a person; if not, it searches for a group authorisation. If there is no group authorisation, the system searches for a role authorisation, then for the client authorisation and finally whether the action is generally available. This means that the person authorisation is the most specific and therefore the strongest authorisation, while the general authorisation is the most general and therefore also the weakest authorisation.